FUJITSU

SPARC Enterprise
M4000/M5000/M8000/M9000 Servers

Administration Guide

C120-E331-03EN

FUJITSU

SPARC® Enterprise M4000/M5000/M8000/M9000 Servers Administration Guide

Manual Code C120-E331-03EN
Part No. 819-7892-10
April 2007, Revision A

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

FUJITSU LIMITED provided technical input and review on portions of this material.

Sun Microsystems, Inc. and Fujitsu Limited each own or control intellectual property rights relating to products and technology described in this document, and such products, technology and this document are protected by copyright laws, patents and other intellectual property laws and international treaties. The intellectual property rights of Sun Microsystems, Inc. and Fujitsu Limited in such products, technology and this document include, without limitation, one or more of the United States patents listed at http://www.sun.com/patents and one or more additional patents or patent applications in the United States or other countries.

This document and the product and technology to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of such product or technology, or of this document, may be reproduced in any form by any means without prior written authorization of Fujitsu Limited and Sun Microsystems, Inc., and their applicable licensors, if any. The furnishing of this document to you does not give you any rights or licenses, express or implied, with respect to the product or technology to which it pertains, and this document does not contain or represent any commitment of any kind on the part of Fujitsu Limited or Sun Microsystems, Inc., or any affiliate of either of them.

This document and the product and technology described in this document may incorporate third-party intellectual property copyrighted by and/or licensed from suppliers to Fujitsu Limited and/or Sun Microsystems, Inc., including software and font technology.

Per the terms of the GPL or LGPL, a copy of the source code governed by the GPL or LGPL, as applicable, is available upon request by the End User. Please contact Fujitsu Limited or Sun Microsystems, Inc.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, Netra, Solaris, Sun Ray, Answerbook2, docs.sun.com, OpenBoot, and Sun Fire are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited.

All SPARC trademarks are used under license and are registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

SPARC64 is a trademark of SPARC International, Inc., used under license by Fujitsu Microelectronics, Inc. and Fujitsu Limited.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

United States Government Rights - Commercial use. U.S. Government users are subject to the standard government user license agreements of Sun Microsystems, Inc. and Fujitsu Limited and the applicable provisions of the FAR and its supplements.

Disclaimer: The only warranties granted by Fujitsu Limited, Sun Microsystems, Inc. or any affiliate of either of them in connection with this document or any product or technology described herein are those expressly set forth in the license agreement pursuant to which the product or technology is provided. EXCEPT AS EXPRESSLY SET FORTH IN SUCH AGREEMENT, FUJITSU LIMITED, SUN MICROSYSTEMS, INC. AND THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND (EXPRESS OR IMPLIED) REGARDING SUCH PRODUCT OR TECHNOLOGY OR THIS DOCUMENT, WHICH ARE ALL PROVIDED AS IS, AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Unless otherwise expressly set forth in such agreement, to the extent allowed by applicable law, in no event shall Fujitsu Limited, Sun Microsystems, Inc. or any of their affiliates have any liability to any third party under any legal theory for any loss of revenues or profits, loss of use or data, or business interruptions, or for any indirect, special, incidental or consequential damages, even if advised of the possibility of such damages.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Please
Recycle

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Entrée et revue tecnical fournies par FUJITSU LIMITED sur des parties de ce matériel.

Sun Microsystems, Inc. et Fujitsu Limited détiennent et contrôlent toutes deux des droits de propriété intellectuelle relatifs aux produits et technologies décrits dans ce document. De même, ces produits, technologies et ce document sont protégés par des lois sur le copyright, des brevets, d'autres lois sur la propriété intellectuelle et des traités internationaux. Les droits de propriété intellectuelle de Sun Microsystems, Inc. et Fujitsu Limited concernant ces produits, ces technologies et ce document comprennent, sans que cette liste soit exhaustive, un ou plusieurs des brevets déposés aux États-Unis et indiqués à l'adresse http://www.sun.com/patents de même qu'un ou plusieurs brevets ou applications brevetées supplémentaires aux États-Unis et dans d'autres pays.

Ce document, le produit et les technologies afférents sont exclusivement distribués avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit, de ces technologies ou de ce document ne peut être reproduite sous quelque forme que ce soit, par quelque moyen que ce soit, sans l'autorisation écrite préalable de Fujitsu Limited et de Sun Microsystems, Inc., et de leurs éventuels bailleurs de licence. Ce document, bien qu'il vous ait été fourni, ne vous confère aucun droit et aucune licence, expresses ou tacites, concernant le produit ou la technologie auxquels il se rapporte. Par ailleurs, il ne contient ni ne représente aucun engagement, de quelque type que ce soit, de la part de Fujitsu Limited ou de Sun Microsystems, Inc., ou des sociétés affiliées.

Ce document, et le produit et les technologies qu'il décrit, peuvent inclure des droits de propriété intellectuelle de parties tierces protégés par copyright et/ou cédés sous licence par des fournisseurs à Fujitsu Limited et/ou Sun Microsystems, Inc., y compris des logiciels et des technologies relatives aux polices de caractères.

Par limites du GPL ou du LGPL, une copie du code source régi par le GPL ou LGPL, comme applicable, est sur demande vers la fin utilsateur disponible; veuillez contacter Fujitsu Limted ou Sun Microsystems, Inc.

Cette distribution peut comprendre des composants développés par des tierces parties.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, Netra, Solaris, Sun Ray, Answerbook2, docs.sun.com, OpenBoot, et Sun Fire sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Fujitsu et le logo Fujitsu sont des marques déposées de Fujitsu Limited.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

SPARC64 est une marques déposée de SPARC International, Inc., utilisée sous le permis par Fujitsu Microelectronics, Inc. et Fujitsu Limited.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une license non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Droits du gouvernement américain - logiciel commercial. Les utilisateurs du gouvernement américain sont soumis aux contrats de licence standard de Sun Microsystems, Inc. et de Fujitsu Limited ainsi qu'aux clauses applicables stipulées dans le FAR et ses suppléments.

Avis de non-responsabilité: les seules garanties octroyées par Fujitsu Limited, Sun Microsystems, Inc. ou toute société affiliée de l'une ou l'autre entité en rapport avec ce document ou tout produit ou toute technologie décrit(e) dans les présentes correspondent aux garanties expressément stipulées dans le contrat de licence régissant le produit ou la technologie fourni(e). SAUF MENTION CONTRAIRE EXPRESSÉMENT STIPULÉE DANS CE CONTRAT, FUJITSU LIMITED, SUN MICROSYSTEMS, INC. ET LES SOCIÉTÉS AFFILIÉES REJETTENT TOUTE REPRÉSENTATION OU TOUTE GARANTIE, QUELLE QU'EN SOIT LA NATURE (EXPRESSE OU IMPLICITE) CONCERNANT CE PRODUIT, CETTE TECHNOLOGIE OU CE DOCUMENT, LESQUELS SONT FOURNIS EN L'ÉTAT. EN OUTRE, TOUTES LES CONDITIONS, REPRÉSENTATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON, SONT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE. Sauf mention contraire expressément stipulée dans ce contrat, dans la mesure autorisée par la loi applicable, en aucun cas Fujitsu Limited, Sun Microsystems, Inc. ou l'une de leurs filiales ne sauraient être tenues responsables envers une quelconque partie tierce, sous quelque théorie juridique que ce soit, de tout manque à gagner ou de perte de profit, de problèmes d'utilisation ou de perte de données, ou d'interruptions d'activités, ou de tout dommage indirect, spécial, secondaire ou consécutif, même si ces entités ont été préalablement informées d'une telle éventualité.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Preface xvii

1. Introduction to Server Software and Configuration 1

XSCF Firmware 1

Solaris OS Software 2

Software Services 3

Preparing for System Configuration 4

Information Needed 4

Initial Configuration Tasks 5

Related Information 5

2. Access Control 7

About Access Control 7

Logging in to the System 8

XSCF User Accounts 8

XSCF Passwords 9

Privileges 9

XSCF Firmware Update 11

XSCF Shell Procedures for Access Control 11

▼ To Log in Initially to the XSCF Console 12

▼ To Add an XSCF User Account 14
▼ To Create a Password for an XSCF User 14
▼ To Configure an XSCF Password Policy 14
▼ To Assign Privileges to an XSCF User 15
▼ To Display the Version of Installed Firmware 15
Related Information 16

3. System Configuration 17

About System Services 17
DSCP Network Between a Service Processor and a Domain 18
XSCF Network Interfaces 19
Domain Name Service 21
LDAP Service 21
Time Synchronization and NTP Service 23
SNMP Service 24
Additional Services 25
HTTPS Service 26
Telnet Service 26
SMTP Service 26
SSH Service 26
Altitude Setting 26
XSCF Shell Procedures for System Configuration 27
▼ To Configure the DSCP Network 28
▼ To Display DSCP Network Configuration 29
▼ To Configure the XSCF Network Interfaces 29
▼ To Configure the XSCF Network Route Information 30
▼ To Set Or Reset the XSCF Network 31
▼ To Display XSCF Network Configuration 31
▼ To Set the Service Processor Host Name and DNS Domain Name 32

- To Set the Service Processor's DNS Name Server 33
- To Enable or Disable Use of an LDAP Server for Authentication and Privilege Lookup 33
- To Configure the Service Processor as an LDAP Client 34
- To Set the NTP Configuration 34
- To Display the NTP Configuration 35
- To Set the Timezone, Daylight Saving Time, Date, and Time Locally on the Service Processor 35
- To Create a USM User Known to the SNMP Agent 36
- To Display USM Information for the SNMP Agent 37
- To Create a VACM Group 38
- To Create a VACM View 38
- To Give a VACM Group Access to a VACM View 38
- To Display VACM Information for the SNMP Agent 39
- To Configure the SNMP Agent to Send Version 3 Traps to Hosts 39
- To Enable the SNMP Agent 40
- To Display SNMP Agent Configuration 40
- To Enable or Disable the Service Processor HTTPS Service 41
- To Enable or Disable the Service Processor Telnet Service 42
- To Configure the Service Processor SMTP Service 42
- To Enable or Disable the Service Processor SSH Service 42
- To Generate a Host Public Key for SSH Service 43
- To Set the Altitude on the Service Processor 43

Related Information 44

4. Domain Configuration 45

About Domains 45

Domains and System Boards 46

Domain Resource Assignment 50

Domain Component List and Logical System Boards 51

Overview of Steps for Domain Configuration 51

Domain Configuration Example 52

Domain Communication 54

DSCP Network 55

Accessing a Domain Console from the Service Processor 55

Logging in Directly to a Domain 55

DVD Drive or Tape Drive Assignment 55

Backup and Restore Operations 56

Dynamic Reconfiguration 56

XSCF Shell Procedures for Domain Configuration 56

- To Specify the XSB Mode 56
- To Set Up a Domain Component List 57
- To Assign an XSB to a Domain 57
- To Power On a Domain 57
- To Display System Board Status 58
- To Access a Domain From the XSCF Console 58
- To Attach a DVD or Tape Drive While the Solaris OS Is Running (M8000/M9000 Servers) 59
- To Disconnect a DVD or Tape Drive While the Solaris OS Is Running (M8000/M9000 Servers) 59

Related Information 61

5. Audit Configuration 63

About Auditing 63

Audit Records 64

Audit Events 64

Audit Classes 65

Audit Policy 65

Audit File Tools 65

XSCF Shell Procedures for Auditing 66

▼ To Enable or Disable Writing of Audit Records to the Audit Trail 66
▼ To Configure an Auditing Policy 66
▼ To Display Whether Auditing is Enabled Or Disabled 67
▼ To Display Current Auditing Policy, Classes, or Events 67
Related Information 67

6. Log Archiving Facility 69

About Log Archiving 69
Using the Log Archiving Facility 69
Archive Host Requirements 71
Log Archiving Errors 71
Using the `snapshot` Tool 71
Solaris OS Procedures for Log Archiving 72
▼ To Configure the Log Archive Host 72
XSCF Shell Procedures for Log Archiving 72
▼ To Enable Log Archiving 72
▼ To Disable Log Archiving 73
▼ To Display Log Archiving Configuration and Status 73
▼ To Display Log Archiving Error Details 73
Related Information 74

7. Capacity on Demand 75

About Capacity on Demand 75
COD Boards 76
COD License Purchase 76
License Installation 77
License Allocation 77
Headroom Management 78
License Violations 79

XSCF Shell Procedures for Using COD 79

- To Install a COD License 79
- To Delete a COD License 80
- To Reserve Licenses for Allocation 81
- To Increase or Decrease Headroom 82
- To Disable Headroom 83
- To Display COD Information 83
- To Display COD License Status 84
- To Display Usage Statistics for COD Resources 85

Related Information 87

A. Mapping Device Path Names 89

Glossary 99

Index 103

Figures

FIGURE 2-1 Location of the Operator Panel MODE Switch on a Midrange Server 12

FIGURE 2-2 Operator Panel on a High-end Server 13

FIGURE 3-1 Relationship of the Service Processor and the DSCP Network to the Domains 18

FIGURE 4-1 A Physical System Board in Uni-XSB Mode on an M4000 Midrange Server 46

FIGURE 4-2 A Physical System Board in Uni-XSB Mode on a High-End Server 47

FIGURE 4-3 A Physical System Board in Quad-XSB Mode on a Midrange Server 48

FIGURE 4-4 A Physical System Board in Quad-XSB Mode on a High-End Server 48

FIGURE 4-5 Example of XSBs and Solaris Domains on a High-End Server 49

FIGURE 6-1 Log Archiving 70

Tables

TABLE 1-1 Software Services 3

TABLE 2-1 User Privileges 10

TABLE 3-1 XSCF Network Interfaces 20

TABLE 3-2 LDAP LDIF File Attributes 22

TABLE 3-3 XSCF and Domain Time Synchronization 23

TABLE 4-1 Boards, Domains, and Domain ID Numbers 49

TABLE 4-2 Resource Assignment in Quad-XSB Mode on an M4000 Midrange Server 50

TABLE 4-3 Resource Assignment in Quad-XSB Mode on an M5000 Midrange Server 50

TABLE 4-4 Resource Assignment in Quad-XSB Mode on a High-end Server 51

TABLE A-1 LSB Numbers and Starting Processor Numbers 90

TABLE A-2 LSB Numbers and Device Path Values 92

TABLE A-3 I/O Device Mapping on a Midrange Server 93

TABLE A-4 Internal Devices and Device Paths on the M4000 and M5000 Servers 93

TABLE A-5 Internal Devices and Device Paths on the M5000 Server 94

TABLE A-6 I/O Device Mapping on a High-end Server 94

TABLE A-7 Internal Devices and Device Paths on a High-end Server 95

TABLE A-8 `cfgadm` Device Matrix for Midrange Servers 97

TABLE A-9 `cfgadm` Device Matrix for High-End Servers 98

Code Samples

CODE EXAMPLE 3-1 LDAP Schema 22

CODE EXAMPLE 3-2 Sample LDAP LDIF File Attributes 22

CODE EXAMPLE 3-3 Sample `ntp.conf` File for a Domain using XSCF as NTP Server 24

Preface

The SPARC Enterprise M4000/M5000/M8000/M9000 Servers Administration Guide describes the system configuration procedures, which focuses on the initial settings of the SPARC Enterprise M4000/M5000/M8000/M9000 servers. This document describes the settings of service processors which embedded in the SPARC Enterprise M4000/M5000/M8000/M9000 servers and also refers to the settings of the Solaris™ Operating System, accompanied by the service processors settings.

This document targets at every model of the SPARC Enterprise M4000/M5000/M8000/M9000 servers; however, in some parts, describes the content specific to the model, such as the midrange (SPARC Enterprise M4000/M5000) servers or the high-end (SPARC Enterprise M8000/M9000) servers. Please refer to the part relevant to the model in use.

To better understand the content of this document, it is recommended to read the following manuals together.

- About the hardware:
  The *SPARC Enterprise M8000/M9000 Servers Overview Guide* or the *SPARC Enterprise M4000/M5000 Servers Overview Guide*
- About the eXtended System Control Facility (XSCF) firmware in the service processor:
  SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide
  SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF Reference Manual

This section includes:

- "Audience" on page xviii"
- "Structure and Contents of This Manual" on page xviii
- "SPARC Enterprise Mx000 Servers Documentation" on page xix
- "Abbreviated References to Other Documents" on page xxii
- "Models" on page xxiii
- "Text Conventions" on page xxiii
- "Prompt Notations" on page xxiv
- "Syntax of the Command Line Interface (CLI)" on page xxiv
- "Software License" on page xxv

■ "Fujitsu Welcomes Your Comments" on page xxv

Audience

This manual is intended for users, who administrate SPARC Enterprise M4000/M5000/M8000/M9000 servers (hereinafter referenced to as XSCF user). The XSCF user is required to have the following knowledge:

- Solaris™ Operating System and Unix command
- SPARC Enterprise M4000/M5000/M8000/M9000 servers and basic knowledge of XSCF

Structure and Contents of This Manual

This manual is organized as described below:

- Chapter 1

  This chapter provides an introduction to the system software and configuration.

- Chapter 2

  This chapter describes access control, including log in, user accounts, passwords, and privileges.

- Chapter 3

  This chapter describes initial configuration of services and networks.

- Chapter 4

  This chapter contains information on domains and domain communication.

- Chapter 5

  This chapter describes auditing functionality.

- Chapter 6

  This chapter describes the log archiving feature.

- Chapter 7

  This chapter covers capacity on demand (COD) and licenses.

- Appendix A

This appendix contains information on mapping device path names.

Glossary and Index

- Glossary

  The glossary explains the terms used in this manual

- Index

  The index provides keywords and corresponding reference page numbers so that the reader can easily search for items in this manual as necessary.

SPARC Enterprise M*x*000 Servers Documentation

The manuals listed below are provided for reference.

Book Titles	Manual Codes
SPARC Enterprise M4000/M5000 Servers Site Planning Guide	C120-H015
SPARC Enterprise M8000/M9000 Servers Site Planning Guide	C120-H014
SPARC Enterprise Equipment Rack Mounting Guide	C120-H016
SPARC Enterprise M4000/M5000 Servers Getting Started Guide	C120-E345
SPARC Enterprise M8000/M9000 Servers Getting Started Guide	C120-E323
SPARC Enterprise M4000/M5000 Servers Overview Guide	C120-E346
SPARC Enterprise M8000/M9000 Servers Overview Guide	C120-E324
Important Safety Information for Hardware Systems	C120-E391
SPARC Enterprise M4000/M5000 Servers Safety and Compliance Guide	C120-E348
SPARC Enterprise M8000/M9000 Servers Safety and Compliance Guide	C120-E326
SPARC Enterprise M4000 Server Unpacking Guide	C120-E349
SPARC Enterprise M5000 Server Unpacking Guide	C120-E350
SPARC Enterprise M8000/M9000 Servers Unpacking Guide	C120-E327
SPARC Enterprise M4000/M5000 Servers Installation Guide	C120-E351
SPARC Enterprise M8000/M9000 Servers Installation Guide	C120-E328

Book Titles	Manual Codes
SPARC Enterprise M4000/M5000 Servers Service Manual	C120-E352
SPARC Enterprise M8000/M9000 Servers Service Manual	C120-E330
External I/O Expansion Unit Installation and Service Manual	C120-E329
SPARC Enterprise M4000/M5000/M8000/M9000 Servers RCI Build Procedure	C120-E361
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Administration Guide	C120-E331
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	C120-E332
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF Reference Manual	C120-E333
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Dynamic Reconfiguration (DR) User's Guide	C120-E335
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide	C120-E336
SPARC Enterprise M4000/M5000/M8000/M9000 Servers RCI User's Guide	C120-E360
SPARC Enterprise M4000/M5000 Servers Product Notes	C120-E347
SPARC Enterprise M8000/M9000 Servers Product Notes	C120-E325

1. Manuals on the Web

   The latest versions of all the SPARC Enterprise Series manuals are available at the following websites. The latest manuals can be downloaded in a batch.

   Global Site

   http://www.fujitsu.com/sparcenterprise/manual/

   Japanese Site

   http://primeserver.fujitsu.com/sparcenterprise/manual/

Note – Product Notes is available on the website only. Please check for the recent update on your product.

2. Documentation CD

   For the Documentation CD, please contact your local sales representative.

   - SPARC Enterprise M4000/M5000 Servers Documentation CD (C120-E365)
   - SPARC Enterprise M8000/M9000 Servers Documentation CD (C120-E364)

3. Manual included on the Enhanced Support Facility x.x CD-ROM disk

- Remote maintenance service

Book Title	Manual Code
Enhanced Support Facility User's Guide for REMCS	C112-B067

4. Provided in system

   Man page of the XSCF

Note – The man page can be referenced on the XSCF Shell, and it provides the same content as the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF Reference Manual*.

5. Documentation and Supporting on the Web

   The latest information about other documents and the supporting of the SPARC Enterprise series are provided on the website.

   a. Message

      http://www.fujitsu.com/sparcenterprise/msg/

   b. Downloading the firmware program

      Contact the field engineer.

      The following files or document are provided.

      i. Firmware program file (XSCF Control Package (XCP) file)

      ii. XSCF extension MIB definition file

Note – XSCF Control Package (XCP) : XCP is a package which has the control programs of hardware that configures a computing system. The XSCF firmware and the OpenBoot PROM firmware are included in the XCP file.

   c. Fault Management MIB (SUN-FM-MIB) definition file

      http://src.opensolaris.org/source/xref/onnv/onnv-gate/usr/src/lib/fm/libfmd_snmp/mibs/

   d. Solaris Operating System Related Manuals

      http://docs.sun.com

6. Provided In firmware program CD (For maintenance service <for FEs>)

      i. Firmware program file (XSCF Control Package (XCP) file)

      ii. XSCF extension MIB definition file

7. Information on Using the RCI function

   The manual does not contain an explanation of the RCI build procedure. For information on using the RCI function, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers RCI Build Procedure* and the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers RCI User's Guide* available on the website.

Abbreviated References to Other Documents

In this manual, the following abbreviated titles may be used when referring to a systems manual. The following table lists the abbreviations used in this manual.

Abbreviated Title	Full Title
Overview Guide	SPARC Enterprise M4000/M5000 Servers Overview Guide SPARC Enterprise M8000/M9000 Servers Overview Guide
Service Manual	SPARC Enterprise M4000/M5000 Servers Service Manual SPARC Enterprise M8000/M9000 Servers Service Manual
Installation Guide	SPARC Enterprise M4000/M5000 Servers Installation Guide SPARC Enterprise M8000/M9000 Servers Installation Guide
Administration Guide	SPARC Enterprise M4000/M5000/M8000/M9000 Servers Administration Guide
XSCF Reference Manual	SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF Reference Manual
Dynamic Reconfiguration User's Guide	SPARC Enterprise M4000/M5000/M8000/M9000 Servers Dynamic Reconfiguration (DR) User's Guide

Models

The model names used in this manual are as follows.

Server class	Model name
Midrange	SPARC Enterprise M4000 SPARC Enterprise M5000
High-end	SPARC Enterprise M8000 SPARC Enterprise M9000

Text Conventions

This manual uses the following fonts and symbols to express specific types of information.

Fonts/symbols	Meaning	Example
AaBbCc123	What you type, when contrasted with on-screen computer output	# **ls -l** <Return>
AaBbCc123	The names of commands, files, and directories; on-screen computer output	# ls -l <Return>
Italic	Indicates the name of a reference manual	See the *XSCF User's Guide*.
" "	Indicates names of chapters, sections, items, buttons, or menus	See Chapter 2, "Access Control."

Prompt Notations

The following prompt notations are used in this manual.

Shell	Prompt Notations
XSCF	XSCF>
C shell	*machine-name*%
C shell super user	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell super user	#
OpenBoot PROM	ok

Syntax of the Command Line Interface (CLI)

The command syntax is described below.

Command syntax

The command syntax is as follows:

- A variable that requires input of a value must be enclosed in <>.
- An optional element must be enclosed in [ ].
- A group of options for an optional keyword must be enclosed in [ ] and delimited by |.
- A group of options for a mandatory keyword must be enclosed in {} and delimited by |.
- The command syntax is shown in a box.

Example:

```
XSCF> showuser -a
```

Software License

The function to explain in this manual uses the softwares of GPL,LGPL and others. For the information of the license, see Appendix E, "Software License Condition" in *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*

Fujitsu Welcomes Your Comments

We would appreciate your comments and suggestions to improve this document. You can submit your comments by using "Reader's Comment Form" on page xxvii

Reader's Comment Form

We would appreciate your comments and suggestions for improving this publication.

Date:_____ Publication No.:
Your Name:_____ Publication Name:
Company: _____
Address: _____
City/State/Zip:_____
Phone/Email address: _____

Your Comments:

Page	Line	Comments
Reply requested: o Yes o No		

Please evaluate the overall quality of this manual by checking (✓)the appropriate boxes

	Good	Fair	Poor		Good	Fair	Poor		Good	Fair	Poor
Organization:	o	o	o	Use of examples:	o	o	o	Legibility:	o	o	o
Accuracy:	o	o	o	Index coverage:	o	o	o	Binding:	o	o	o
Clarity:	o	o	o	Cross				Figures and tables:	o	o	o
Overall rating of				referencing:	o	o	o	General appearance:	o	o	o
this publication:	o	o	o								

Technical level: o Too detailed o Appropriate o Not enough detail

All comments and suggestions become the property of Fujitsu Limited.

For Users in U.S.A., Canada, and Mexico

Fold and fasten as shown on back
No postage necessary if mailed in U.S.A.

Fujitsu Computer Systems
Attention: Engineering Ops M/S 249
1250 East Arques Avenue
P.O. Box 3470
Sunnyvale, CA 94088-3470
FAX: (408) 746-6813

For Users in Other Countries

Fax this form to the number below or send this form to the address below.

Fujitsu Learning Media Limited
FAX: 81-3-3730-3702
37-10 Nishi-Kamata 7-chome
Oota-Ku
Tokyo 144-0051
JAPAN

FUJITSU LIMITED

FOLD AND TAPE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO 741 SUNNYVALE CA

POSTAGE WILL BE PAID BY ADDRESSEE

FUJITSU

FUJITSU COMPUTER SYSTEMS
ATTENTION ENGINEERING OPS M/S 249
1250 EAST ARQUES AVENUE
P O BOX 3470
SUNNYVALE CA 94088-3470

FOLD AND TAPE

CHAPTER 1

Introduction to Server Software and Configuration

This chapter provides an overview of the SPARC® Enterprise M4000/M5000/M8000/M9000 server (hereafter referred to as the SPARC Enterprise M*x*000 server) software and configuration. It has these sections:

- XSCF Firmware
- Solaris OS Software
- Software Services
- Preparing for System Configuration
- Related Information

Note – This manual documents both the midrange (M4000 and M5000) and the high-end (M8000 and M9000) SPARC Enterprise M*x*000 server. This manual covers initial system configuration only. (See "Initial Configuration Tasks" on page 5.) When you have completed the initial configuration, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide* for day-to-day system administration and management tasks.

XSCF Firmware

A SPARC Enterprise M*x*000 server provides system management capabilities through eXtended System Controller Facility (XSCF) firmware, pre-installed at the factory on the Service Processor[1] boards.

XSCF firmware consists of system management applications and two user interfaces to configure and control them:

1. The Service Processor is sometimes referred to as the XSCF Unit, or XSCFU.

- XSCF Web, a browser-based graphical user interface
- XSCF Shell, a terminal-based command-line interface

You can access the XSCF firmware by logging in to the XSCF command shell. This document includes instructions for using the XSCF interface as part of the initial system configuration. For more information about the XSCF firmware, refer to Chapter 2 and to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

XSCF firmware, OpenBoot™ PROM firmware, and power-on self-test (POST) firmware are known collectively as the XSCF Control Package (XCP).

XSCF firmware has two networks for internal communication. The Domain to Service Processor Communications Protocol (DSCP) network provides an internal communication link between the Service Processor and the Solaris domains. The XSCF network provides an internal communication link between the two Service Processors in a high-end SPARC Enterprise M*x*000 server.

On a high-end server with two Service Processors, one Service Processor is configured as *active* and the other is configured as *standby*. This redundancy of two Service Processors allows them to exchange system management information and, in case of failover, to change roles. All configuration information on the active Service Processor is available to the standby Service Processor.

Solaris OS Software

The Solaris OS is pre-installed at the factory on one domain by default in a SPARC Enterprise M*x*000 server. Within its domain, the Solaris OS includes features to manage Solaris OS system capabilities.

You can install applications on the domains. That process is managed through the Solaris OS tools. Likewise, any other software management applications that you prefer to use on the domains must be installed through the Solaris OS tools.

The DSCP network provides an internal communication link between the Service Processor and the Solaris domains.

Software Services

TABLE 1-1 contains an overview of software services and networks that are part of a SPARC Enterprise M*x*000 server, and where they are documented.

TABLE 1-1 Software Services

Service	Description
Access control	Access control includes logging in to the system, user accounts, passwords, privileges, and XSCF firmware control. Refer to Chapter 2.
Initial system configuration	Initial configuration of the services for the Service Processor and the domains, including DSCP network, XSCF network, DNS name service, LDAP service, NTP service, HTTPS service, Telnet service, SSH service, SNMP service, and SMTP service. Refer to Chapter 3.
Domain configuration	Each domain in a SPARC Enterprise M*x*000 server runs its own copy of the Solaris OS. Domains are managed by the Service Processor XSCF firmware, and communicate with the Service Processor over the DSCP network. You can access a domain console from the Service Processor or, if your system is networked, log in to a domain directly. Refer to Chapter 4.
Auditing	The auditing function logs all security-related events on a SPARC Enterprise M*x*000 server. Refer to Chapter 5.
Log archiving	The log archiving function allows you to set up a remote host to automatically receive and store log data from a SPARC Enterprise M*x*000 server. Refer to Chapter 6.
Capacity on demand (COD)	Capacity on Demand is an option that allows you to purchase spare processing capacity for a SPARC Enterprise M*x*000 server. The spare capacity is provided in the form of one or more CPUs on COD boards that are installed on your server. To use the CPU processing capacity, you must purchase a license. The XSCF firmware allows you to set up and manage COD. Refer to Chapter 7.
Security	Security is provided through access control (user names, passwords, privileges), audit logs of security-related events, and various security protocols. A SPARC Enterprise M*x*000 server is secure by default. That is, other than setting up user accounts and privileges, no initial configuration has to be done related to security. For example, no insecure protocols, such as Telnet, are initially enabled. Refer to Chapter 2, Chapter 5.

TABLE 1-1 Software Services *(Continued)*

Service	Description
Fault management	No initial configuration is needed. • Domain fault management includes CPU, memory, and I/O (PCI/PCIe) nonfatal errors. All nonfatal errors are reported to the Solaris OS, which will attempt to take faulty CPUs offline or to retire faulty memory pages. Fatal errors are generally handled by the Service Processor. • Service Processor fault management includes fatal CPU, memory, and I/O errors (the Service Processor will exclude the faulty components upon reboot), as well as environmental monitoring (power supplies, fan speeds, temperatures, currents) and the External I/O Expansion Unit. Refer to the Solaris OS documentation collection.
Hot-replacement operations	No initial configuration is needed. PCI cards can be removed and inserted in a SPARC Enterprise M*x*000 server while the system continues to operate. The Solaris OS `cfgadm` command is used to unconfigure and disconnect a PCI card. Refer to the *Service Manual;* Solaris OS documentation collection.
External I/O Expansion Unit management	No initial configuration is needed. The External I/O Expansion Unit is a rack mountable PCI card chassis. Refer to the *External I/O Expansion Unit Installation and Service Manual.*

Preparing for System Configuration

This section lists the information needed for initial system configuration and the initial configuration tasks.

Information Needed

Before you configure the software, have the following available:

- Access to the Service Processor with the appropriate privileges for your tasks.

  More information about access is contained in Chapter 2.
- An unused range of IP addresses for the internal DSCP network between the Service Processor and the domains.
- Network configuration information for the Service Processor, including IP addresses, netmask, DNS server, default route, NFS server.

- The number of domains in your system. By default, there is one domain and its domain number is 0 (zero). The number of domains could be different from the default if you specified another number of domains when you ordered your system.
- Firmware version information if you are upgrading the XSCF firmware.
- Information for optional services that you are going to use, such as Lightweight Directory Access Protocol (LDAP) information for authentication.

Initial Configuration Tasks

Initial configuration requires these tasks:

1. Logging in to the Service Processor with the default log-in name over a serial connection. You must have physical access to the system.
2. Adding at least one user account with a minimum of one privilege, `useradm`. This user with `useradm` privileges can then create the rest of the user accounts.
3. Configuring the DSCP network.
4. Configuring the XSCF network.
5. Setting the Service Processor time. The Service Processor can be an NTP client, or an NTP client and NTP server for the domains.
6. Configuring or enabling any optional services you want to use immediately.

   These services include Telnet, SNMP, SMTP, LDAP, NTP, HTTPS, DNS, SSH, domains, log archiving, and COD.

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages (see Note following this table)	`fmdump`(8), `fmadm`(8), `fmstat`(8), `version`(8), `cfgadm`(1M)
Site Planning Guide	Site planning
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	System configuration and administration

Resource	Information
Solaris OS documentation collection	Solaris OS, including fault management
Service Manual	Hot-replacement operations, fault management
External I/O Expansion Unit Installation and Service Manual	PCI card chassis

Note – `man` pages available on the Service Processor are followed by (8), for example, `version`(8); they are also available in the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF Reference Manual*. Solaris OS `man` pages available on the domains are followed by (1M), for example, `cfgadm`(1M).

CHAPTER 2

Access Control

Access control is a way of granting access to the system functions or components only to those users who have been authenticated by the system and who have appropriate *privileges*. Access control depends on the proper configuration of the general security services provided by the SPARC Enterprise M*x*000 server.

This chapter contains these sections:

- About Access Control
- XSCF Shell Procedures for Access Control
- Related Information

About Access Control

The Service Processor is a SPARC Enterprise M*x*000 server *appliance*. In an appliance model, users or management agents can access the Service Processor and its components only through authorized user interfaces. Users and agents cannot access any of the underlying operating system interfaces, and users cannot install individual software components on the Service Processor.

These sections provide details on access control:

- Logging in to the System
- XSCF User Accounts
- XSCF Passwords
- Privileges
- XSCF Firmware Update

Logging in to the System

There are two entities that can be logged in to on the system, a Service Processor and a Solaris domain.

You initially log in to the Service Processor using a serial connection from a terminal device. A terminal device can be an ASCII terminal, a workstation, or a PC. For details on serial port connections, see the *Installation Guide* for your server or the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

A unique login account with the user name of `default` exists on the Service Processor. This account is unique in the following ways:

- It can never be logged in to using the standard UNIX user name and password authentication or SSH public key authentication.
- It can only be logged in to using a procedure that requires physical access to the system.
- Its privileges are fixed to be `useradm` and `platadm`; you cannot change these privileges.
- It cannot be deleted, it has no password, and no password can be set for it.

After initial configuration, you can log in to the Service Processor using a serial connection or an Ethernet connection. You can redirect the XSCF console to a domain and get a Solaris console. You can also log in to a domain directly using an Ethernet connection to access the Solaris OS.

When a user logs in, the user establishes a *session*. Authentication and user privileges are valid only for that session. When the user logs out, that session ends. To log back in, the user must be authenticated once again, and will have the privileges in effect during the new session. See "Privileges" on page 9 for information on privileges.

XSCF User Accounts

A user account is a record of an individual user that can be verified through a user name and password.

When you initially log in to the system, add at least one user account with a minimum of one privilege, `useradm`. This user with `useradm` privileges can then create the rest of the user accounts. For a secure log in method, enable SSH service. Refer to "To Enable or Disable the Service Processor SSH Service" on page 42 and to "To Generate a Host Public Key for SSH Service" on page 43 for more information.

XSCF supports multiple user accounts for log in to the Service Processor. The user accounts are assigned privileges; each privilege allows the user to execute certain XSCF commands. By specifying privileges for each user, you can control which

operations each XSCF user is allowed to perform. On its own, a user account has no privileges. To obtain permission to run XSCF commands and access system components, a user must have privileges.

You can set up the Service Processor to use an LDAP server for authentication instead. To use LDAP, the Service Processor must be set up as an LDAP client. For information about setting up the Service Processor to use the LDAP service, refer to "LDAP Service" on page 21. If you are using an LDAP server for authentication, the user name must not be in use, either locally or in LDAP.

XSCF Passwords

User passwords are authenticated locally by default unless you are using an LDAP server for authentication.

Site-wide policies, such as password nomenclature or expiration dates, make passwords more difficult to guess. You can configure a password policy for the system using the `setpasswordpolicy` command. The `setpasswordpolicy` command describes the default values for a password policy.

If you have lost password access to your system, use the procedure "To Log in Initially to the XSCF Console" on page 12.

Privileges

Privileges allow a user to perform a specific set of actions on a specific set of components. Those components can be physical components, domains, or physical components within a domain.

The system provides the predefined privileges shown in TABLE 2-1. These are the only privileges allowed in a SPARC Enterprise M*x*000 server. You cannot define additional privileges.

TABLE 2-1 User Privileges

Privilege	Capabilities
`none`	None. When the local privilege for a user is set to `none`, that user has no privileges, even if privileges for that user are defined in LDAP. Setting a user's local privilege to `none` prevents the user's privileges from being looked up in LDAP.
`useradm`	Can create, delete, disable, and enable user accounts. Can change a user's password and password properties. Can change a user's privileges. Can view all platform states.
`platadm`	Can perform all Service Processor configuration other than the `useradm` and `auditadm` tasks. Can assign and unassign hardware to or from domains. Can perform domain and Service Processor power operations. Can perform Service Processor failover operations on systems with more than one Service Processor. Can perform all operations on domain hardware. Can view all platform states.
`platop`	Can view all platform states.
`domainadm`	Can perform all operations on hardware assigned to the domain(s) on which this privilege is held. Can perform all operations on the domain(s) on which this privilege is held. Can view all states of the hardware assigned to the domain(s) on which this privilege is held. Can view all states of the domain(s) on which this privilege is held.
`domainmgr`	Can perform domain power operations. Can view all states of the hardware assigned to the domain(s) on which this privilege is held. Can view all states of the domain(s) on which this privilege is held.
`domainop`	Can view all states of the hardware assigned to the domain(s) on which this privilege is held. Can view all states of the domain(s) on which this privilege is held.
`auditadm`	Can configure auditing. Can delete audit trail.
`auditop`	Can view all audit states and the audit trail.
`fieldeng`	Can perform all operations reserved for field engineers.

The `domainadm`, `domainmgr`, and `domainop` privileges must include the domain number, numbers, or range of numbers to associate with a particular user account.

A user can have multiple privileges, and a user can have privileges on multiple domains.

User privileges are authenticated locally by default. You can set up the Service Processor to use an LDAP server for authentication instead. For information about setting up the Service Processor to use the LDAP service, refer to "LDAP Service" on page 21.

If no privileges are specified for a user, no local privilege data will exist for that user; however, the user's privileges can be looked up in LDAP, if LDAP is being used. If a user's privileges are set to `none`, that user does not have any privileges, regardless of privilege data in LDAP.

XSCF Firmware Update

The Service Processor firmware can only be updated as an entire *image*, known as an XCP image. The image includes the XSCF firmware, OpenBoot PROM firmware, POST firmware, and miscellaneous files. Only valid images authorized by Sun Microsystems or Fujitsu can be installed.

The XCP image is installed in the Service Processor flash memory. You need `platadm` or `fieldeng` privilege to update an XCP image. More information on updating an XCP image is contained in the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

XSCF Shell Procedures for Access Control

This section describes these procedures:

- To Log in Initially to the XSCF Console
- To Add an XSCF User Account
- To Create a Password for an XSCF User
- To Configure an XSCF Password Policy
- To Assign Privileges to an XSCF User
- To Display the Version of Installed Firmware

▼ To Log in Initially to the XSCF Console

This procedure can be used for initial login or for lost password access.

1. **Log in to the XSCF console with the default login name from a terminal device connected to the Service Processor[1]. You must have physical access to the system.**

```
serial port log-in prompt: default
```

You are prompted to toggle the Operator Panel MODE switch (keyswitch) on the front of the system. The location of the MODE switch on a midrange SPARC Enterprise M*x*000 server is shown in FIGURE 2-1. The MODE switch on a high-end SPARC Enterprise M*x*000 server is mounted horizontally rather than vertically, as shown in FIGURE 2-2. The MODE switch has two positions: Service and Locked.

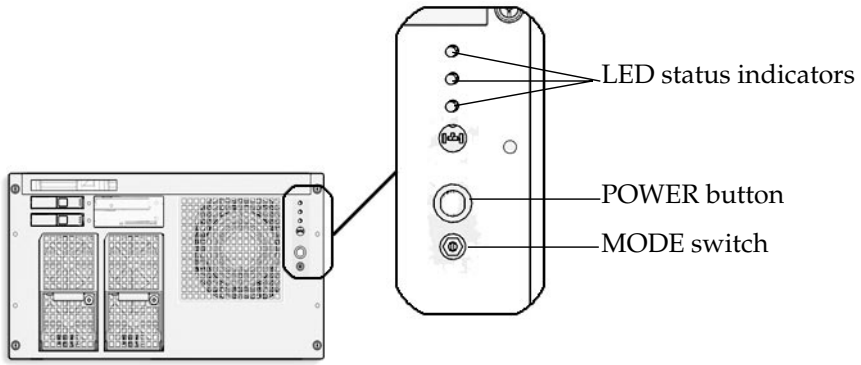

FIGURE 2-1 Location of the Operator Panel MODE Switch on a Midrange Server

1. For details on serial port connections, see the *Installation Guide* for your server or the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

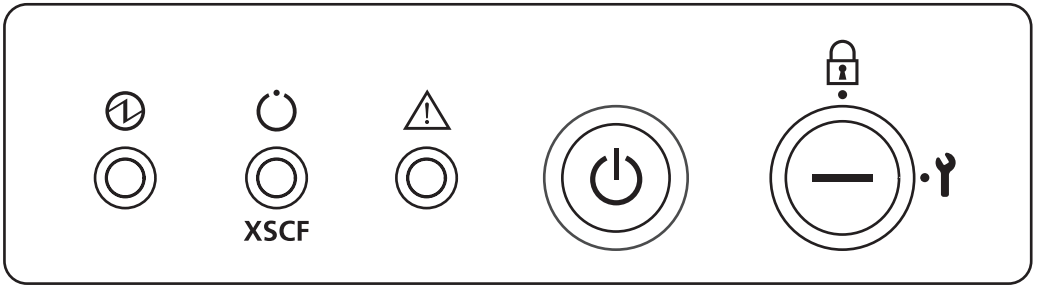

FIGURE 2-2 Operator Panel on a High-end Server

You must toggle the MODE switch within one minute of the login prompt or the login process times out.

2. **Toggle the MODE switch using one of two methods, as follows:**
   - If the switch is in the Service position, turn it to the Locked position, leave it there for at least five seconds, and then turn it back to the Service position. Press the `Enter` key.
   - If the switch is in the Locked position, turn it to the Service position, leave it there for at least five seconds, and then turn it back to the Locked position. Press the `Enter` key.

   When the toggling is successful, you are logged in to the Service Processor shell as the account `default`.

```
XSCF>
```

As this account has `useradm` and `platadm` privileges. you can now configure the Service Processor or reset passwords.

When the shell session ends, the `default` account is disabled. When an account is disabled, it cannot be used to log in at the console. It will then not be possible to login using this account again except by following this same procedure.

▼ To Add an XSCF User Account

When you add a new user account, the account has no password, and cannot be used for logging in until the password is set or Secure Shell public key authentication is enabled for the user.

1. **Log in to the XSCF console with** `useradm` **privileges.**
2. **Type the** `adduser` **command:**

```
XSCF> adduser user
```

where *user* is the user name you want to add. If you do not specify a User ID (UID) number with the `-u UID` option, one is automatically assigned, starting from 100.

3. **Verify that the operation succeeded by typing the** `showuser` **command**.

▼ To Create a Password for an XSCF User

Any XSCF user can set his or her own password. Only a user with `useradm` privileges can set another user's password.

1. **Log in to the XSCF console with** `useradm` **privileges.**
2. **Type the** `password` **command:**

```
XSCF> password
Please enter your password:
```

When typed without an argument, `password` sets the current user's password. To set someone else's password, include their user name, for example:

```
XSCF> password user
Please enter your password:
```

where *user* is the user name you want to set the password for. You are prompted to enter, and then reenter, the password.

▼ To Configure an XSCF Password Policy

1. **Log in to the XSCF console with** `useradm` **privileges.**

2. **Type the** `setpasswordpolicy` **command:**

```
XSCF> setpasswordpolicy option
```

where option can be one or more of the options described in the `setpasswordpolicy`(8) `man` page.

3. **Verify that the operation succeeded by typing the** `showpasswordpolicy` **command**.

▼ To Assign Privileges to an XSCF User

1. **Log in to the XSCF console with** `useradm` **privileges.**
2. **Type the** `setprivileges` **command:**

```
XSCF> setprivileges user privileges
```

where *user* is the user name to assign privileges for, and *privileges* is one or more privileges, separated by a space, to assign to this user. The `domainadm`, `domainmgr`, and `domainop` privileges must include the domain number, numbers, or range of numbers to associate with a particular user account; for example,

```
XSCF> setprivileges user domainadm@1-4, 6, 9
```

Valid privileges are listed in TABLE 2-1.

▼ To Display the Version of Installed Firmware

1. **Log in to the XSCF console with** `platadm` **or** `fieldeng` **privileges.**

2. **Type the** `version` **command:**

```
XSCF> version -c xcp
```

The XCP version number is displayed. Command output example is:

```
XSCF> version -c xcp
XSCF#0(Active)
XCP0 (Current): 1020
...
```

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages	`password`(8), `version`(8), `adduser`(8), `deleteuser`(8), `enableuser`(8), `disableuser`(8), `showuser`(8), `setpasswordpolicy`(8), `setprivileges`(8), `showpasswordpolicy`(8), `setlookup`(8), `setldap`(8), `showldap`(8)
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	Access control, user accounts, passwords, firmware update

CHAPTER 3

System Configuration

This chapter describes how to initially configure system services and internal networks that enable communication between the components of your SPARC Enterprise M*x*000 server.

This chapter contains these sections:

- About System Services
- XSCF Shell Procedures for System Configuration
- Related Information

About System Services

A SPARC Enterprise M*x*000 server uses various services to enable communication between its components. Refer to "Preparing for System Configuration" on page 4 for an overview of initial service configuration.

These sections provide details on system services:

- DSCP Network Between a Service Processor and a Domain
- XSCF Network Interfaces
- Domain Name Service
- LDAP Service
- Time Synchronization and NTP Service
- SNMP Service
- Additional Services

DSCP Network Between a Service Processor and a Domain

The Domain to Service Processor Communications Protocol (DSCP) service provides a secure TCP/IP- and PPP-based communication link between the Service Processor and each domain. Without this link, the Service Processor cannot communicate with the domains.

The Service Processor requires one IP address dedicated to the DSCP service on its side of the link, and one IP address on *each* domain's side of the link. The DSCP service is a point-to-point link between the Service Processor and each domain. FIGURE 3-1 illustrates this relationship.

.

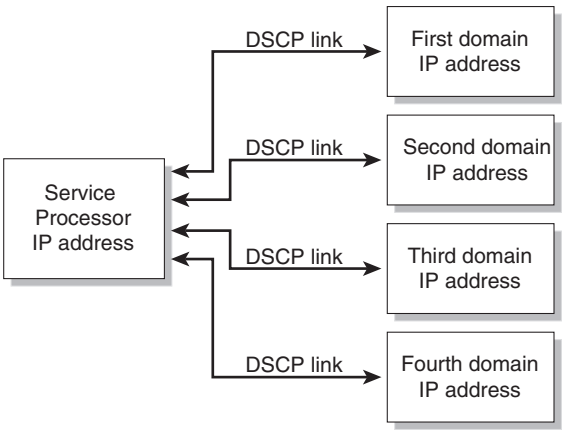

FIGURE 3-1 Relationship of the Service Processor and the DSCP Network to the Domains

DSCP service is not configured by default. You configure and use the service by specifying IP addresses for the Service Processor and the domains. The IP addresses should be nonroutable addresses on the network.

The `setdscp` command provides an interactive mode that displays a prompt for each DSCP setting you can configure:

- The network address to be used by the DSCP network for IP addresses
- The netmask for the DSCP network
- The Service Processor IP address
- An IP address for each domain

In a system with redundant Service Processors, the standby Service Processor does not communicate with the domains. In the event of a failover, the newly active Service Processor assumes the IP address of the failed-over Service Processor.

DSCP includes its own security measures that prohibit a compromised domain from compromising other domains or the Service Processor.

The DSCP should only be configured when there are no domains running. If you change the DSCP configuration while a domain is active, you have to power off the domain before the Service Processor can communicate with it. Refer to Chapter 4 for more information on domains.

In a typical DSCP configuration, you enter a network address and netmask using the `setdscp` command. The system then configures the Service Processor IP address and any domain IP addresses according to this formula: the Service Processor gets an IP address that is the network address +1; and each domain gets an IP address that is the Service Processor IP address, + the domain ID, +1. For example, if you enter 10.1.1.0 for the network address, and 255.255.255.0 for the netmask, the `showdscp` command displays output similar to the following:

```
XSCF> showdscp
DSCP Configuration:
Network: 10.1.1.0
Netmask: 255.255.255.0

Location     Address
XSCF         10.1.1.1
Domain #00   10.1.1.2
Domain #01   10.1.1.3
Domain #02   10.1.1.4
Domain #03   10.1.1.5
...
```

This scenario minimizes the range of IP addresses needed for DSCP.

XSCF Network Interfaces

The XSCF network configurable settings include the IP address for the active Service Processor, IP address for the standby Service Processor, gateway address, netmask, and network route.

TABLE 3-1 lists the XSCF network interfaces.

TABLE 3-1 XSCF Network Interfaces

XSCF Unit	Interface Name	Description
XSCF Unit 0 (midrange server and high-end server)	`xscf#0-lan#0`	XSCF LAN#0 (external)
	`xscf#0-lan#1`	XSCF LAN#1 (external)
	`xscf#0-if`	Interface between XSCF Units (internal)
XSCF Unit 1 (high-end server)	`xscf#1-lan#0`	XSCF LAN#0 (external)
	`xscf#1-lan#1`	XSCF LAN#1 (external)
	`xscf#1-if`	Interface between XSCF Units (internal)
	`lan#0`	Takeover IP address for XSCF LAN#0
	`lan#1`	Takeover IP address for XSCF LAN#1

On a high-end server, one Service Processor is configured as *active* and the other is configured as *standby*. The XSCF network between the two Service Processors allows them to exchange system management information and, in case of failover, to change roles.

Optionally, a "floating" IP address can be set up, which is hosted on the currently active Service Processor. External clients can use this floating IP address to connect to whichever Service Processor is active. Selection of a floating IP address does not affect failover.

When you set or change the information related to the XSCF network, including the Service Processor host name, DNS domain name, DNS server, IP address, netmask, or routing information, you must make the changes effective in XSCF and reset the Service Processor. This is done with the `applynetwork` command.

You configure the XSCF network with these commands:

- `setnetwork`
- `setroute`
- `sethostname` (if using DNS)
- `setnameserver` (if using DNS)
- `applynetwork`

Once you have configured the XSCF network, it requires no day-to-day management.

Domain Name Service

The Domain Name Service (DNS) allows computers on a network to communicate with each other by using centrally maintained DNS names instead of locally stored IP addresses. If you configure the Service Processor to use the DNS service, it "joins" the DNS community and can communicate with any other computer on the network through its DNS server.

There are no defaults for this service. To configure the Service Processor to use DNS, you must specify the Service Processor host name, and the DNS server name and IP address.

You can configure the Service Processor DNS service with these commands:

- `sethostname`
- `setnameserver`

On a server with dual Service Processors, the domain name is common for both Service Processors. A host name can be specified for each Service Processor. Setting a different host name for each Service Processor does not disable failover.

Once you have configured the Service Processor to use the DNS service, it does not require day-to-day management.

LDAP Service

The LDAP service stores user authentication and privilege settings on a server so that individual computers on the network do not have to store the settings.

By default, the Service Processor stores user passwords and privileges locally. Account information for users who have access to the Service Processor are stored on the Service Processor itself. (Authentication and privilege lookups for the server's domains are provided by the Solaris OS.)

However, if you want to have authentication and privilege lookups performed by an LDAP server, you can set up the Service Processor to be an LDAP client.

The general process for setting up the Service Processor as an LDAP client is:

1. Enable the LDAP service.
2. Provide the LDAP server configuration information:
   - The IP address or hostname, and port, of the primary LDAP directory
   - *Optional:* The IP address or hostname, and port, of up to two alternative LDAP directories
   - The distinguished name (DN) of the search base to use for lookup

- Whether Transport Layer Security (TLS) is to be used

3. Verify that the LDAP service is working.

On the LDAP server, you create an LDAP schema with privilege properties. The schema contains the following:

CODE EXAMPLE 3-1 LDAP Schema

```
attributetype ( 1.3.6.1.1.1.1.40 NAME 'spPrivileges'
   DESC 'Service Processor privileges'
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
   SINGLE-VALUE )

objectclass ( 1.3.6.1.1.1.2.13 NAME 'serviceProcessorUser' SUP top
AUXILIARY
   DESC 'Service Processor user'
   MAY spPrivileges )
```

You also add the following required attributes for each user on the LDAP server, as shown in TABLE 3-2.

TABLE 3-2 LDAP LDIF File Attributes

Field Name	Description
`spPrivileges`	A valid privilege on the Service Processor
`homeDirectory`	The location of the home directory on the Service Processor: `/scf/home`
`loginShell`	The login shell on the Service Processor: `/scf/bin/rbash`
`uidNumber`	The user ID number on the Service Processor. The `uidnumber` must be greater than 100. Use the `showuser` command to display UIDs.

A sample file entry is:

CODE EXAMPLE 3-2 Sample LDAP LDIF File Attributes

```
spPrivileges: platadm
homeDirectory: /scf/home
loginShell: /scf/bin/rbash
uidNumber: 150
```

Refer to the Solaris OS documentation collection for more information on LDAP servers.

If the LDAP client is configured and enabled on the Service Processor, lookups are first performed locally, and then through the LDAP server. If no privileges are specified for a user, the `setprivileges` command deletes any local privilege data for that user. Subsequently, the user's privileges will be looked up in LDAP, if LDAP privilege lookup is enabled. If the `none` privilege is specified for a user, that user will not have any privileges, regardless of privilege data in LDAP.

These commands manage the Service Processor LDAP service:

- `setlookup`
- `setldap`

Note that passwords stored in the LDAP repository must use either UNIX crypt or MD5 encryption schemes.

Once you have configured the Service Processor to use the LDAP service, it does not require day-to-day management.

Time Synchronization and NTP Service

The Network Time Protocol (NTP) provides the correct timestamp for all systems on a network by synchronizing the clocks of all the systems. NTP service is provided by an NTP daemon.

To use the NTP service, the Service Processor can be set up as an NTP client, using the services of a remote NTP server, or it can be set up as an NTP server and client itself. TABLE 3-3 shows how the time is synchronized.

TABLE 3-3 XSCF and Domain Time Synchronization

Entity	Primary NTP Server	Time Synchronization Method
XSCF	No connection	The XSCF time is the time in the initial system setting or the time set with the `setdate` command.
	External NTP server	XSCF operates as an NTP client. The XSCF time is adjusted to the time of the external NTP server.
Domain	XSCF	XSCF operates as the NTP server. The domain time is adjusted to the time of the XSCF.
	External NTP server	The domain time is adjusted to the time of the external NTP server.

When domains are powered on, they synchronize their clocks to the XSCF clock, or to an external NTP server.

If the domain and the Service Processor are using the same time source (for example, the Service Processor), one benefit is that events logged in the Solaris OS and on the Service Processor can be correlated based on their timestamp; if the domain uses a different server as the NTP server, the Service Processor and domain times may drift, and correlating log files could become difficult.

Every NTP server and every NTP client must have an `ntp.conf` file, in `/etc/inet/ntp.conf`. The Service Processor has a default `ntp.conf` file. If you are using NTP, you must create an `ntp.conf` file on each domain.

If you are using the Service Processor as the NTP server for the domains, create an `ntp.conf` file on each domain similar to the following:

CODE EXAMPLE 3-3 Sample `ntp.conf` File for a Domain using XSCF as NTP Server

```
server ip_address
slewalways yes
disable pll
enable auth monitor
driftfile /var/ntp/ntp.drift
statsdir /var/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
```

where *ip_address* is the IP address you configured for the Service Processor on the DSCP network. To display the Service Processor's IP address, use the `showdscp -s` command.

If you are using an external NTP server for the domains, refer to the `xntpd`(1M) `man` page or to the Solaris OS documentation collection for information on creating the `ntp.conf` file for each domain.

SNMP Service

A Simple Network Management Protocol (SNMP) agent can be configured and enabled on the Service Processor. The Service Processor SNMP agent monitors the state of the system hardware and domains, and exports the following information to an SNMP manager:

- System information such as chassis ID, platform type, total number of CPUs, and total memory
- Configuration of the hardware
- Dynamic reconfiguration information, including which domain-configurable units are assigned to which domains
- Domain status

- Power status
- Environmental status

The Service Processor SNMP agent can supply system information and fault event information using public MIBs. SNMP managers, for example, a third-party manager application, use any Service Processor network interface with the SNMP agent port to communicate with the agent. The SNMP agent supports concurrent access from multiple users through SNMP managers.

By default, the SNMP agent uses version 3 (v3) of the SNMP protocol. SNMP v3 is secure, requiring an authentication protocol, authentication password, and encryption password. The valid authentication protocols are MD5 and SHA (secure hash algorithm). You can also configure your server to accept earlier SNMP versions 1 and 2.

The SNMP agent includes the v3 utilities for user management, the User Security Model (USM), and for view access control, the View Access Control Model (VACM). You can change the configuration of SNMP agent traps, USM user accounts, and VACM information.

Initial SNMP v3 configuration includes:

1. Creating USM user information
2. Creating VACM access control information (group, view, and access)

   Using VACM requires a basic knowledge of SNMP and MIBs. Refer to the *Solaris System Management Agent Administration Guide* and to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide* for information.
3. Configuring the SNMP agent
4. Enabling the SNMP agent
5. Setting up your SNMP manager application to communicate with the Service Processor SNMP agent based on the configuration you used for the agent, namely, user, port, and trap information.

The SNMP agent is active only on the active Service Processor. In the event of failover, the SNMP agent is restarted on the newly active Service Processor.

Additional Services

This section describes HTTPS, Telnet, SMTP, and SSH services, and altitude settings.

This section does not cover all the optional services and settings for the Service Processor that you might want to set up and use at a later date. For example, you can set up mirrored memory mode on the Service Processor using the `setupfru` command. Refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide* for information on day-to-day administration and management tasks.

HTTPS Service

Hypertext Transfer Protocol (HTTP) over an authenticated/encrypted connection allows you to use the XSCF web browser securely. This is called the HTTPS service. Authentication is provided with a certificate authority and private keys. To use the HTTPS service, you must enable it, and provide an optional port number. The default port is 443. To enable HTTPS service, use the `sethttps` command.

Telnet Service

Telnet service is disabled by default on the Service Processor. To enable it, use the `settelnet` command. Telnet provides an alternative for those sites that do not have `ssh`.

SMTP Service

Simple Mail Transfer Protocol (SMTP) service is controlled by these commands:

- `showsmtp`
- `setsmtp`

The authentication mechanisms allowed by the mail server are `pop`, `smtp-auth`, or `none` (the default). The SMTP authentications supported are `plain` and `login`.

SSH Service

SSH service is disabled by default. To enable it, use the `setssh` command. A host public key is required for SSH service.

Altitude Setting

The altitude for your server is 0 meters by default. You can set the altitude using the `setaltitude` command. If the altitude is set, any abnormality in the intake air temperature can be detected quickly. However, even if no altitude is set, any

abnormality in the air temperature, such as the CPU temperature, can still be detected. The server temperature limits are set to protect the domain hardware, so this command is logically used before powering on any domain.

XSCF Shell Procedures for System Configuration

This section describes these procedures:

- To Configure the DSCP Network
- To Display DSCP Network Configuration
- To Configure the XSCF Network Interfaces
- To Configure the XSCF Network Route Information
- To Set Or Reset the XSCF Network
- To Display XSCF Network Configuration
- To Set the Service Processor Host Name and DNS Domain Name
- To Set the Service Processor's DNS Name Server
- To Enable or Disable Use of an LDAP Server for Authentication and Privilege Lookup
- To Configure the Service Processor as an LDAP Client
- To Set the NTP Configuration
- To Display the NTP Configuration
- To Set the Timezone, Daylight Saving Time, Date, and Time Locally on the Service Processor
- To Create a USM User Known to the SNMP Agent
- To Display USM Information for the SNMP Agent
- To Create a VACM Group
- To Create a VACM View
- To Give a VACM Group Access to a VACM View
- To Display VACM Information for the SNMP Agent
- To Configure the SNMP Agent to Send Version 3 Traps to Hosts
- To Enable the SNMP Agent
- To Display SNMP Agent Configuration
- To Enable or Disable the Service Processor HTTPS Service
- To Enable or Disable the Service Processor Telnet Service
- To Configure the Service Processor SMTP Service
- To Enable or Disable the Service Processor SSH Service
- To Generate a Host Public Key for SSH Service

▼ To Configure the DSCP Network

1. **Log in to the XSCF console with** `platadm` **or** `fieldeng` **privileges.**
2. **Type the** `setdscp` **command.**

   You can use one of two methods, as follows:

   - Use the `setdscp` command with the `-y -i` *address* `-m` *netmask* options:

   ```
   XSCF> setdscp -y -i address -m netmask
   ```

   For example:

   ```
   XSCF> setdscp -y -i 10.1.1.0 -m 255.255.255.0
   ```

   - Use the `setdscp` command with no options (interactive mode).

     You are prompted to enter all the DSCP IP addresses sequentially. A command output example of this interactive mode is:

   ```
   XSCF> setdscp
   DSCP network [0.0.0.0]  > 10.1.1.0
   DSCP netmask [255.0.0.0]  > 255.255.255.0
   XSCF address [10.1.1.1] > [Enter]
   Domain #00 address [10.1.1.2]  > [Enter]
   Domain #01 address [10.1.1.3]  > [Enter]
   Domain #02 address [10.1.1.4]  > [Enter]
   Domain #03 address [10.1.1.5]  > [Enter]
   Domain #04 address [10.1.1.6]  > [Enter]
   Domain #05 address [10.1.1.7]  > [Enter]
   Domain #06 address [10.1.1.8]  > [Enter]
   Domain #07 address [10.1.1.9]  > [Enter]
   Domain #08 address [10.1.1.10] > [Enter]
   ...
   Commit these changes to the database (y|n) ?
   ```

   i. **For each prompt, press the** `Enter` **key to accept the displayed value, or type a new value followed by the** `Enter` **key.**

   ii. **To save your changes, enter** `Y`**. To cancel the changes, enter** `N`**.**

3. **Verify the operation with the** `showdscp` **command.**

▼ To Display DSCP Network Configuration

1. **Log in to the XSCF console with** `platadm`**,** `platop`**, or** `fieldeng` **privileges, or** `domainadm`**,** `domainop`**, or** `domainmgr` **privileges for a specific domain.**
2. **Type the** `showdscp` **command:**

```
XSCF> showdscp
```

Command output example for a DSCP network of 10.1.1.0 and a DSCP netmask of 255.255.255.0 is:

```
XSCF> showdscp
DSCP Configuration:
Network: 10.1.1.0
Netmask: 255.255.255.0

Location     Address
XSCF         10.1.1.1
Domain #00   10.1.1.2
Domain #01   10.1.1.3
Domain #02   10.1.1.4
Domain #03   10.1.1.5
...
```

▼ To Configure the XSCF Network Interfaces

Settings to configure the XSCF network must be applied to XSCF, and the Service Processor must be reset, before the settings become effective. See "To Set Or Reset the XSCF Network" on page 31.

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setnetwork` **command:**

a. To set the network interface, netmask, and IP address:

```
XSCF> setnetwork interface [-m addr] address
```

where *interface* specifies the network interface to be set, -m *addr* specifies the netmask address of the network interface, and *address* specifies the IP address of the network interface. If the `-m` option is omitted, the netmask corresponding to the IP address is set. Refer to TABLE 3-1 for valid interface names.

The following example sets the IP address and netmask for the interface XSCF-LAN#0 on XSCF Unit 1 in a high-end server:

```
XSCF> setnetwork xscf#1-lan#0 -m 255.255.255.0 192.168.11.10
```

b. To enable the specified network interface:

```
XSCF> setnetwork -c [up|down] interface
```

where `-c` specifies whether to enable or disable the specified network interface, and *interface* specifies the network interface to be enabled.

For additional information on the `setnetwork` command, including specifying takeover IP addresses, refer to the `setnetwork`(8) `man` page or to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

3. **Verify the operation with the `shownetwork` command.**

▼ To Configure the XSCF Network Route Information

Settings to configure the XSCF network must be applied to XSCF, and the Service Processor must be reset, before the settings become effective. See "To Set Or Reset the XSCF Network" on page 31.

1. **Log in to the XSCF console with `platadm` privileges.**

2. **Type the** `setroute` **command:**

```
XSCF> setroute -c [add|del] -n address [-m address] [-g address] interface
```

where `-c` specifies whether to add or delete routing information, `-n` *address* specifies the IP address to which routing information is forwarded, `-m` *address* specifies the netmask address to which routing information is forwarded, `-g` *address* specifies the gateway address, and *interface* specifies the network interface to be set with routing information. Refer to TABLE 3-1 for valid interface names.

For additional information on the `setroute` command, including specifying takeover IP addresses, refer to the `setroute`(8) `man` page or to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

▼ To Set Or Reset the XSCF Network

When you set or change the Service Processor host name, DNS domain name, DNS server, IP address, netmask, or routing information, the settings must be applied to XSCF, and the Service Processor must be reset, before the settings become effective.

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `applynetwork` **command:**

```
XSCF> applynetwork
```

The `applynetwork` command displays the information that has been set for the XSCF network, and asks you to reset the Service Processor. The Service Processor must be reset for settings to become effective.

3. **Verify the operation with the** `shownetwork` **command.**

▼ To Display XSCF Network Configuration

1. **Log in to the XSCF console.**

2. **Type the** `shownetwork` **command:**

```
XSCF> shownetwork -a | interface
```

where `-a` displays information for all XSCF network interfaces, and *interface* displays information for a specific XSCF network interface name, in the format `xscf#`*x*`-`*y*.

Command output example for the XSCF Unit #0, LAN#1 is:

```
XSCF> shownetwork xscf#0-lan#1
Link encap:Ethernet HWaddr 00:00:00:12:34:56
inet addr:192.168.10.11 Bcast:192.168.10.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
...
```

▼ To Set the Service Processor Host Name and DNS Domain Name

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `sethostname` **command:**

   a. **To set the Service Processor host name:**

```
XSCF> sethostname xscfu hostname
```

   where *xscfu* can be `xscf#0` (XSCF Unit 0) or `xscf#1` (XSCF Unit 1 in a high-end server); *hostname* is the host name to be set for the specified Service Processor (XSCF Unit).

   b. **To set the Service Processor domain name:**

```
XSCF> sethostname -d domainname
```

3. **To verify the operation, type the** `showhostname` **command.**

```
XSCF> showhostname -a | xscfu
```

where `-a` displays the host names for all XSCF Units, and *xscfu* displays information for a specific XSCF Unit, either `xscf#0` or `xscf#1`.

▼ To Set the Service Processor's DNS Name Server

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setnameserver` **command, followed by one or more IP addresses separated by a comma:**

```
XSCF> setnameserver ip_address
```

3. **To verify the operation, type the** `shownameserver` **command.**

```
XSCF> shownameserver
```

▼ To Enable or Disable Use of an LDAP Server for Authentication and Privilege Lookup

1. **Log in to the XSCF console with** `useradm` **privileges.**
2. **Type the** `setlookup` **command:**

```
XSCF> setlookup -a local|ldap
XSCF> setlookup -p local|ldap
```

The `-a` option sets the authentication lookup to either local or in LDAP; the `-p` option sets the privileges lookup to either local or in LDAP. When `local` is specified, lookup is only done locally; when `ldap` is specified, lookup is first done locally, then in LDAP if not found locally.

3. **To verify the operation, type the** `showlookup` **command.**

```
XSCF> showlookup
```

▼ To Configure the Service Processor as an LDAP Client

Make sure you have added an LDAP privileges schema to the LDAP server, and attributes for each user on the LDAP server. Refer to CODE EXAMPLE 3-1 and CODE EXAMPLE 3-2 for information.

1. **Log in to the XSCF console with** `useradm` **privileges.**
2. **Type the** `setldap` **command:**

```
XSCF> setldap [-b bind] [-B baseDN] [-c certchain] [-p] [-s servers] [-
t user] -T timeout
```

where *bind* is the bind name, *baseDN* is the base Distinguished Name, *certchain* is an LDAP server certificate chain, `-p` sets the password to use when binding to the LDAP server (you are prompted for the password), *servers* sets the primary and secondary LDAP servers and ports, *user* tests the server connection and password for the specified user, and *timeout* is the maximum amount of time allowed for an LDAP search before search results are returned. For more information on LDAP, refer to the `setldap`(8) `man` page, to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*, and to the Solaris OS documentation collection.

3. **To verify the operation, type the** `showldap` **command.**

```
XSCF> showldap
```

▼ To Set the NTP Configuration

If you are using NTP, an `ntp.conf` file must be created on the domains. Refer to "Time Synchronization and NTP Service" on page 23 for information.

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setntp` **command:**

```
XSCF> setntp -c add address
```

where *address* is the IP address of the NTP server.

3. **Reset the Service Processor with the `rebootxscf` command to make the settings effective:**

```
XSCF> rebootxscf
```

4. **To verify the operation, type the `showntp` command.**

```
XSCF> showntp -a
```

▼ To Display the NTP Configuration

1. **Log in to the XSCF console.**
2. **Type the `showntp` command:**

```
XSCF> showntp -a | -l | address
```

where the `-a` option displays all the NTP servers configured for use, the `-l` option displays time synchronization information, and *address* is the IP address of an NTP server to display information for.

▼ To Set the Timezone, Daylight Saving Time, Date, and Time Locally on the Service Processor

1. **Log in to the XSCF console with `platadm` or `fieldeng` privileges.**
2. **Type the `settimezone` command:**

   a. **To display the timezones that you can set:**

```
XSCF> settimezone -c settz -a
```

b. To set the timezone:

```
XSCF> settimezone -c settz -s timezone
```

where *timezone* is the timezone you want to set. For more information on the `settimezone` command, including setting Daylight Saving Time, refer to the `settimezone`(8) `man` page or to the *Reference Manual.*

3. **To verify the operation, type the** `showtimezone` **command.**

```
XSCF> showtimezone
```

4. **Type the** `setdate` **command:**

```
XSCF> setdate -s date
```

where *date* is the date and time you want to set. For more information on the `setdate` command, refer to the `setdate`(8) `man` page or to the *Reference Manual.*

5. **After specifying the date, you are prompted to reset the Service Processor, so that the date and time become effective. Type** `Y` **to reset the Service Processor.**

6. **To verify the operation, type the** `showdate` **command.**

```
XSCF> showdate
```

▼ To Create a USM User Known to the SNMP Agent

A USM user known to the SNMP agent is not required to have a regular user account on the Service Processor.

1. **Log in to the XSCF console with** `platadm` **privileges.**

2. **Type the** `setsnmpusm` **command.**

You can use one of two methods to add USM users, as follows:

- To add a new user, use the `create` argument:

```
XSCF> setsnmpusm create -a authentication_protocol [-p authentication_password]
[-e encryption_password] user
```

where *authentication_protocol* is either MD5 or SHA, *authentication_password* is the authentication password (must be equal to or greater than 8 characters), *encryption_password* is the encryption password, and *user* is the user name to be known to the agent for subsequent SNMP communication. If you do not specify the passwords, you are prompted to enter them.

- To add a new user with the same settings as an existing user, use the `clone` argument:

```
XSCF> setsnmpusm clone -u clone_user user
```

where *clone_user* is a valid user name known to the SNMP agent, and *user* is the user name to be created with the same settings as the valid *clone_user*. Use the `setsnmpusm password` command to change either or both passwords for the cloned user, if desired.

3. **To verify the operation, type the `showsnmpusm` command.**

▼ To Display USM Information for the SNMP Agent

1. **Log in to the XSCF console with `platadm` or `platop` privileges.**
2. **Type the `showsnmpusm` command:**

```
XSCF> showsnmpusm
```

Command output example is:

```
XSCF> showsnmpusm

Username        Auth Protocol
=============   =============
jsmith           SHA
sue              MD5
```

▼ To Create a VACM Group

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setsnmpvacm` **command:**

```
XSCF> setsnmpvacm createview -s OID_subtree [-m OID_Mask] viewname
```

   where *username* is a valid user name known to the SNMP agent, and *groupname* is the name of the group to create for the specified user for view access.

3. **To verify the operation, type the** `showsnmpvacm` **command.**

▼ To Create a VACM View

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setsnmpvacm` **command:**

```
XSCF> setsnmpvacm createview -s OID_subtree [-m OID_Mask] viewname
```

   where *OID_subtree* is the MIB OID subtree for the view (values start at .1 for the entire MIB tree, and can be limited to certain portions of the tree by using the optional *OID_Mask*), and *viewname* is the name of the view to create for the SNMP agent exported MIB information. View access is read-only for the agent.

3. **To verify the operation, type the** `showsnmpvacm` **command.**

▼ To Give a VACM Group Access to a VACM View

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setsnmpvacm` **command:**

```
XSCF> setsnmpvacm createaccess -r viewname groupname
```

   where *viewname* is a valid SNMP agent view, and *groupname* is a valid SNMP agent group name.

3. **To verify the operation, type the** `showsnmpvacm` **command.**

▼ To Display VACM Information for the SNMP Agent

1. **Log in to the XSCF console with** `platadm` **or** `platop` **privileges.**
2. **Type the** `showsnmpvacm` **command:**

```
XSCF> showsnmpvacm
```

Command output example is:

```
XSCF> showsnmpvacm

Groups

Groupname       Username
=============   =============
admin           jsmith, bob

Views

View            Subtree          Mask       Type
=============   =======          ======     =========
all_view        .1               ff         include

Access

View            Group
=============   =============
all_view        admin
```

▼ To Configure the SNMP Agent to Send Version 3 Traps to Hosts

1. **Log in to the XSCF console with** `platadm` **privileges.**

2. **Type the** `setsnmp` **command:**

```
XSCF> setsnmp addv3traphost -u username -r authentication_protocol {-n
engine_id | -i} [-a authentication_password] [-e encryption_password] [-p
trap_port] traphost
```

where *username* is a user known to the SNMP agent, *authentication_protocol* is either MD5 or SHA, *engine_id* is the identifier of the local agent sending the trap, which must match the *engine_id* expected by the host, `-i` asks for acknowledgement from the receiving host, *authentication_password* is the authentication password (must be equal to or greater than 8 characters), *encryption_password* is the encryption password, *trap_port* is the listening port for the SNMP agent (the default is 161), and *traphost* is the host name where the SNMP manager application is running.

If you do not specify the passwords, you are prompted to enter them.

3. **To verify the operation, type the** `showsnmp` **command.**

For additional options with the `setsnmp` command, including information on configuring your system to accept SNMP version 1 or 2 traps, refer to the `setsnmp`(8) `man` page.

▼ To Enable the SNMP Agent

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setsnmp` **command:**

```
XSCF> setsnmp enable
```

3. **To verify the operation, type the** `showsnmp` **command.**

Make sure that your SNMP manager application can communicate with the Service Processor SNMP agent based on the configuration you used for the agent, namely, user, port, and trap information.

▼ To Display SNMP Agent Configuration

1. **Log in to the XSCF console with** `platadm` **or** `platop` **privileges.**

2. **Type the** `showsnmp` **command:**

```
XSCF> showsnmp
```

Command output example is:

```
XSCF> showsnmp

Agent Status:       Enabled
Agent Port:         161
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown

Trap Hosts:

Hostname   Port    Type   Community String  Username  Auth Protocol
--------   ----    ----   ----------------  --------  ------------
host1       162      v3     n/a              user1    SHA

SNMP V1/V2c:         None
```

▼ To Enable or Disable the Service Processor HTTPS Service

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Optionally, display the current status of the Service Processor HTTPS Service:**

```
XSCF> showhttps
```

3. **Type the** `sethttps` **command:**

```
XSCF> sethttps -c function
```

where *function* is either `enable` or `disable`. The HTTPS service starts immediately after being enabled, and stops immediately after being disabled.

For additional options with the `sethttps` command, including information on certificates and private keys, refer to the `sethttps`(8) `man` page or to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

▼ To Enable or Disable the Service Processor Telnet Service

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Optionally, display the current status of the Service Processor Telnet Service:**

```
XSCF> showtelnet
```

3. **Type the** `settelnet` **command:**

```
XSCF> settelnet -c function
```

where *function* is either `enable` or `disable`. The Telnet service starts immediately after being enabled, and stops immediately after being disabled.

▼ To Configure the Service Processor SMTP Service

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Optionally, display the current status of the Service Processor SMTP Service:**

```
XSCF> showsmtp
```

3. **Type the** `setsmtp` **command:**

```
XSCF> setsmtp
```

You are prompted to enter the name of the SMTP mail server to be used, the port number to be used (default is port 25), the authentication mechanism (default is `none`) and the Reply Address. You must specify a valid email address.

▼ To Enable or Disable the Service Processor SSH Service

1. **Log in to the XSCF console with** `platadm` **privileges.**

2. **Optionally, display the current status of the Service Processor SSH Service:**

```
XSCF> showssh
```

3. **Type the** `setssh` **command:**

```
XSCF> setssh -c function
```

where *function* is either `enable` or `disable`. You must generate a host public key to use SSH.

▼ To Generate a Host Public Key for SSH Service

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setssh` **command:**

```
XSCF> setssh -c genhostkey
```

For additional options with the `setssh` command, including information on adding or deleting user public keys, refer to the `setssh`(8) `man` page or to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

▼ To Set the Altitude on the Service Processor

1. **Log in to the XSCF console with** `fieldeng` **privileges.**
2. **Type the** `setaltitude` **command:**

```
XSCF> setaltitude -s altitude=value
```

where *value* is a unit of meters. The unit of meters is rounded off to the nearest hundred meters.

3. **To verify the operation, type the** `showaltitude` **command.**

Related Information

For additional information on this chapter's topics, see:

Resource	Information
man pages	showdscp(8), setdscp(8), shownetwork(8), setnetwork(8), applynetwork(8), showhostname(8), sethostname(8), setroute(8), showroute(8), setdate(8), showdate(8), shownntp(8), setntp(8), xntpd(1M), ntpq(1M), ntpdate(1M), setnameserver(8), shownameserver(8), sethostname(8), showhostname(8), showlookup(8), setlookup(8), showldap(8), setldap(8), showsnmp(8), setsnmp(8), setsnmpusm(8), setsnmpvacm(8), showsnmpusm(8), showsnmpvacm(8), showhttps(8), sethttps(8), showtelnet(8), settelnet(8), showssh(8), setssh(8), showsmtp(8), setsmtp(8), setaltitude(8), showaltitude(8), rebootxscf(8)
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	Topics covered in this chapter and additional information on day-to-day administration
Solaris System Management Agent Administration Guide	SNMP

CHAPTER 4

Domain Configuration

This chapter describes how to set up and manage domains with XSCF firmware. On your server, by default from the factory, there is one domain with the Solaris OS installed, and its Domain Identification Number (DID) is 0 (zero).

This chapter contains these sections:

- About Domains
- XSCF Shell Procedures for Domain Configuration
- Related Information

About Domains

These sections provide details on domain configuration:

- Domains and System Boards
- Domain Resource Assignment
- Domain Component List and Logical System Boards
- Overview of Steps for Domain Configuration
- Domain Configuration Example
- Domain Communication
- DVD Drive or Tape Drive Assignment
- Backup and Restore Operations
- Dynamic Reconfiguration

Domains and System Boards

A domain is an independent system resource that runs its own copy of the Solaris OS. Domains divide a system's total resources into separate units that are not affected by each other's operations. Domains can be used for different types of processing; for example, one domain can be used to test new applications, while another domain can be used for production purposes.

The number of physical system boards in your server varies from 1 to 16, depending on whether you have a midrange or a high-end server. One physical system board (PSB) consists of 4 CPUs, 32 dual inline memory modules (DIMMs), and I/O. The I/O varies with the server, and can include PCIe slots, PCI-X slots, and built-in I/O.

To use a PSB in your system, the hardware resources on the board must be logically divided and reconfigured as eXtended System Boards (XSBs). There are two modes of XSBs:

- Uni-XSB
  - A PSB logically undivided and configured into one XSB
  - Contains all the resources on the board: 4 CPUs, 32 DIMMs, and I/O

  FIGURE 4-1 shows a PSB in Uni-XSB mode on a midrange server, and FIGURE 4-2 shows a PSB in Uni-XSB mode on a high-end server. The CPU modules and memory modules are known as the CPU/memory board unit (CMU) and the I/O devices are contained in the I/O unit (IOU).

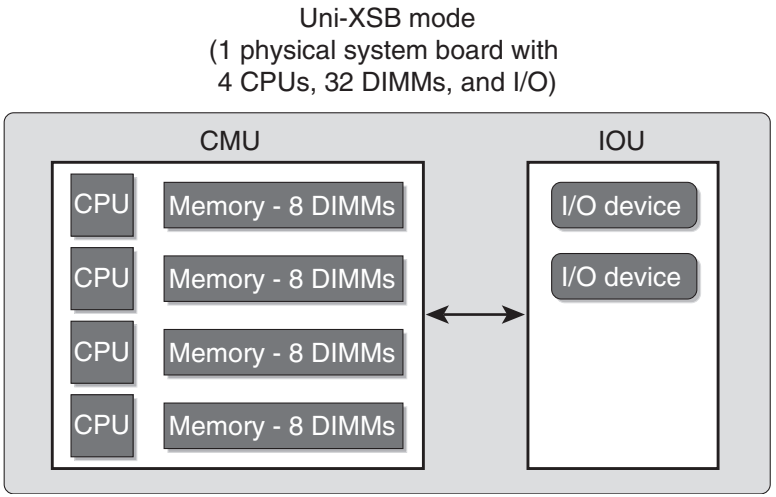

FIGURE 4-1 A Physical System Board in Uni-XSB Mode on an M4000 Midrange Server

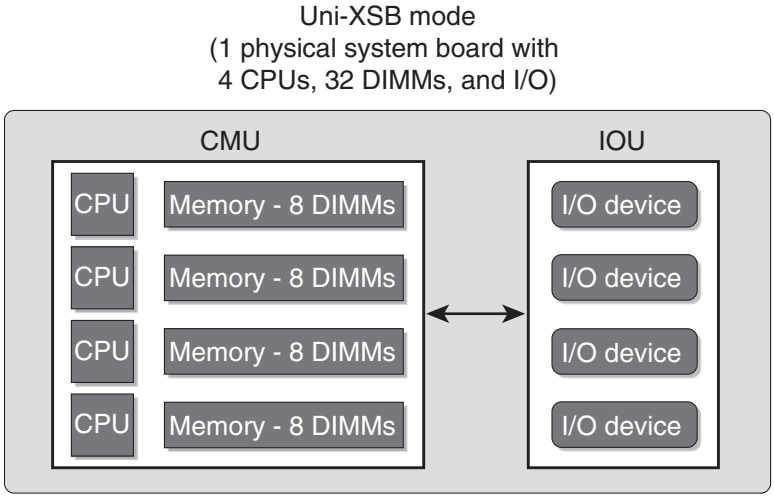

FIGURE 4-2 A Physical System Board in Uni-XSB Mode on a High-End Server

- Quad-XSB
  - A PSB logically divided and configured into four XSBs
  - Each of the four XSBs contains one-quarter of the total board resources: 1 CPU, 8 DIMMs, and I/O. On a midrange server, only two XSBs have I/O.

  FIGURE 4-3 shows a PSB in Quad-XSB mode on a midrange server, and FIGURE 4-4 shows a PSB in Quad-XSB mode on a high-end server.

The logical dividing between Uni-XSB and Quad-XSB is done using the `setupfru` command.

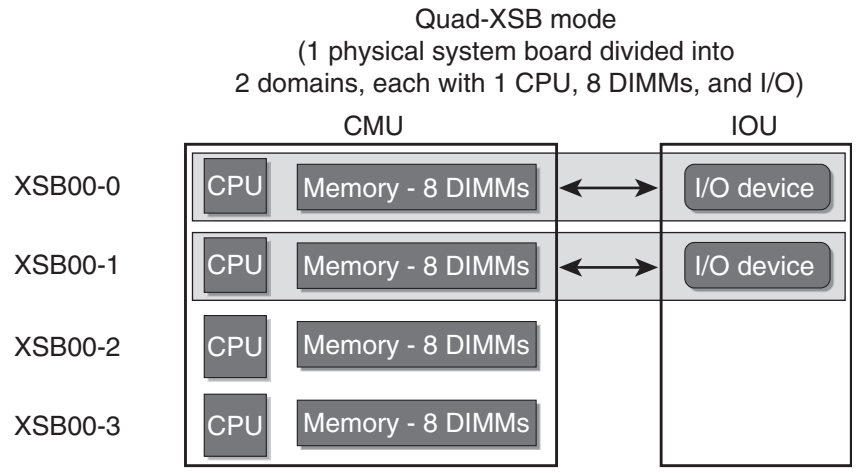

FIGURE 4-3 A Physical System Board in Quad-XSB Mode on a Midrange Server

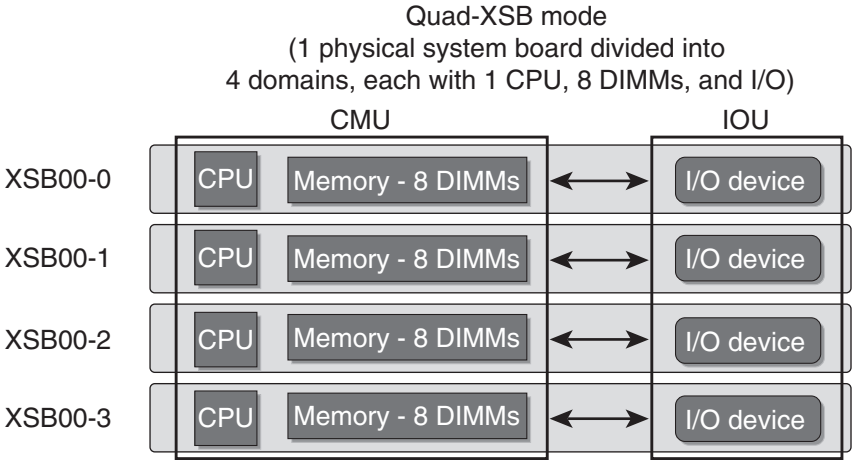

FIGURE 4-4 A Physical System Board in Quad-XSB Mode on a High-End Server

A domain consists of one or more XSBs. Each domain runs its own copy of the Solaris OS. A domain must have, at a minimum, 1 CPU, 8 DIMMs, and I/O.

In FIGURE 4-3, one domain (for example, domain 0) must contain XSB 00-0, and the second domain (for example, domain 1) must contain XSB 00-1, because of the I/O requirement for a domain. The remaining XSB 00-2 and XSB 00-3 can be assigned to either domain, or to none.

The number of domains allowed depends on which midrange or high-end server model you have. The default is one domain and the maximum number of domains is 24. Each domain is identified with a domain ID number, with the default domain as #0.

TABLE 4-1 shows the maximum number of system boards, the maximum number of domains, and the domain ID number range by server model.

TABLE 4-1 Boards, Domains, and Domain ID Numbers

Server Model	Maximum Physical System Boards	Maximum Domains	Domain ID Number Range
M9000 + expansion unit	16	24	0-23
M9000	8	24	0-23
M8000	4	16	0-15
M5000	2	4	0-3
M4000	1	2	0-1

Domains can be set up to include both Uni-XSBs and Quad-XSBs. FIGURE 4-5 shows two XSBs in Uni-XSB mode (left side of figure) and two XSBs in Quad-XSB mode (right side of figure) on a high-end server; the partition of these boards into three Solaris domains is shown by shading.

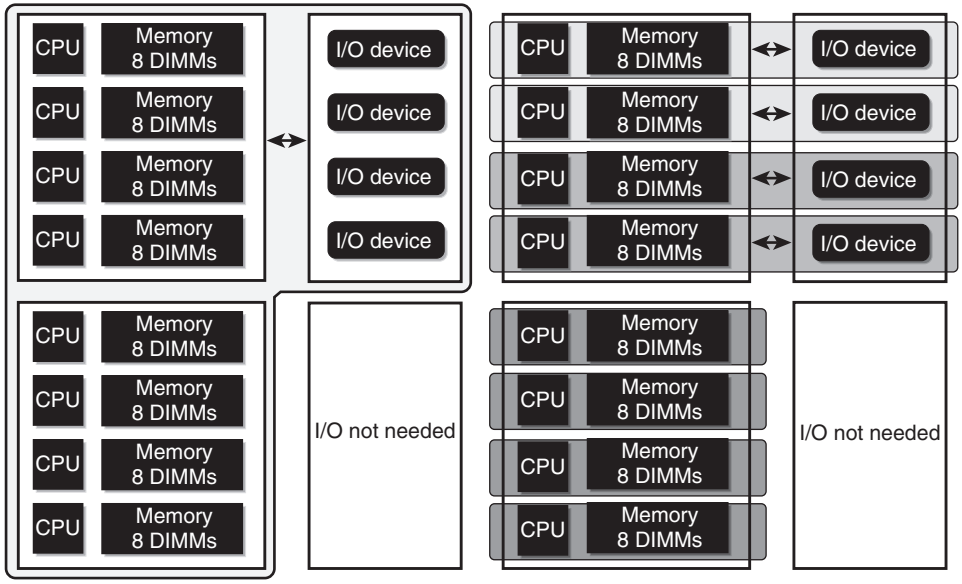

FIGURE 4-5 Example of XSBs and Solaris Domains on a High-End Server

The Solaris OS is installed on a per-domain basis. In the configuration shown in FIGURE 4-5, there would be three Solaris images, one for each domain. The OS image is installed on internal disks. The internal disks are available only for the first (top) I/O device and the third (third from top) I/O device. The second and fourth I/O devices do not have the capability to have internal hard disks.

Domain Resource Assignment

The assignment of CPU modules (CPUM), memory, and I/O to domains in Quad-XSB mode is shown in TABLE 4-2, TABLE 4-3 and TABLE 4-4.

TABLE 4-2 Resource Assignment in Quad-XSB Mode on an M4000 Midrange Server

XSB	CPU	Memory Board	I/O
00-0	CPUM#0-CHIP#0	MEMB#0	Disks; GbE; PCI#0, PCI#1, PCI#2
00-1	CPUM#0-CHIP#1	MEMB#1	PCI#3, PCI#4
00-2	CPUM#1-CHIP#0	MEMB#2	None
00-3	CPUM#1-CHIP#1	MEMB#3	None

TABLE 4-3 Resource Assignment in Quad-XSB Mode on an M5000 Midrange Server

XSB	CPU	Memory Board	I/O
00-0	CPUM#0-CHIP#0	MEMB#0	Disks; GbE; IOU#0-PCI#0, IOU#0-PCI#1, IOU#0-PCI#2
00-1	CPUM#0-CHIP#1	MEMB#1	IOU#0-PCI#3, IOU#0-PCI#4
00-2	CPUM#1-CHIP#0	MEMB#2	None
00-3	CPUM#1-CHIP#1	MEMB#3	None
01-0	CPUM#2-CHIP#0	MEMB#4	Disks; GbE; IOU#1-PCI#0, IOU#1-PCI#1, IOU#1-PCI#2
01-1	CPUM#2-CHIP#1	MEMB#5	IOU#1-PCI#3, IOU#1-PCI#4
01-2	CPUM#3-CHIP#0	MEMB#6	None
01-3	CPUM#3-CHIP#1	MEMB#7	None

In TABLE 4-4, the XSB board number *xx* is in the range of 00-15; the IOU board number *xx* is the IOU board number corresponding to the XSB board number. For example, XSB 00-0 has IOU#00-PCI#0.

TABLE 4-4 Resource Assignment in Quad-XSB Mode on a High-end Server

XSB	CPU	DIMMs	I/O
xx-0	CPUM#0	MEM#00A,B MEM#01A,B MEM#02A,B MEM#03A,B	IOU#*xx*-PCI#0, IOU#*xx*-PCI#1
xx-1	CPUM#1	MEM#10A,B MEM#11A,B MEM#12A,B MEM#13A,B	IOU#*xx*-PCI#2, IOU#*xx*-PCI#3
xx-2	CPUM#2	MEM#20A,B MEM#21A,B MEM#22A,B MEM#23A,B	IOU#*xx*-PCI#4, IOU#*xx*-PCI#5
xx-3	CPUM#3	MEM#30A,B MEM#31A,B MEM#32A,B MEM#33A,B	IOU#*xx*-PCI#6, IOU#*xx*-PCI#7

Domain Component List and Logical System Boards

The domain component list (DCL) identifies the *potential* resources for a domain. A single XSB can potentially belong to multiple domains. However, a single XSB can be *assigned* only to one specific domain.

XSB numbers are not used in domain configuration, however. The software requires that each XSB number "map" to a *logical system board* (LSB) number. Processor numbers and I/O bridges are based on LSB numbers. Appendix A contains additional information on LSB and device path names.

Overview of Steps for Domain Configuration

This section applies to domain configuration after installing a new board in the system.

Note – If you create a new domain, you have to install the Solaris OS on the domain. Refer to the Solaris OS documentation collection for instructions.

Domain configuration typically includes these steps:

1. Log in to the XSCF console with appropriate privileges.
2. Specify the XSB mode, either Uni-XSB or Quad-XSB, using the `setupfru` command.
3. Set up information for a domain (the DCL), using the `setdcl` command. The DCL identifies the potential resources for a domain.
4. Assign the hardware resources (XSBs) to the domain, using the `addboard` command. The DCL must be set up before assigning XSBs to a domain.
5. Power on the domain, using the `poweron` command.

   (Step 5 and Step 6 may be done in reverse order.)
6. Open a console to the domain, using the `console` command.
7. If this is a new domain, at the OpenBoot PROM prompt, install the Solaris OS. Refer to the Solaris OS documentation collection for instructions.
8. Set up any services you want to use on the domain, such as NTP. Refer to Chapter 3 for information on services, including NTP.

Domain Configuration Example

This domain configuration example assumes one PSB in Uni-XSB mode will be set up in Quad-XSB mode and configured into two domains. The domain configuration will be:

domain0 = XSB#00-0 + XSB#00-2

domain1 = XSB#00-1 + XSB#00-3

```
XSCF> setupfru -x 4 sb 0
XSCF> showfru sb 0

Device  Location    XSB Mode        Memory Mirror Mode
sb      00          Quad            no

XSCF> setdcl -d 0 -a 0=00-0
XSCF> setdcl -d 0 -a 1=00-2
```

```
XSCF> addboard -c assign -d 0 00-0 00-2

XSB#00-0 will be assigned to DomainID 0. Continue?[y|n] :y
XSB#00-2 will be assigned to DomainID 0. Continue?[y|n] :y

XSCF> showdcl -v -d 0

DID   LSB   XSB   Status   No-Mem   No-IO    Float    Cfg-policy

00                Powered Off                         FRU
      00    00-0           False    False    False
      01    00-2           False    False    False
      02    -
      03    -
      04    -
      05    -
      06    -
      07    -
      08    -
      09    -
      10    -
      11    -
      12    -
      13    -
      14    -
      15    -

XSCF> poweron -d 0

DomainIDs to power on:0
Continue? [y|n] :y
00 :Powered on

XSCF> setdcl -d 1 -a 0=00-1
XSCF> setdcl -d 1 -a 1=00-3
XSCF> addboard -c assign -d 1 00-1 00-3

XSB#00-1 will be assigned to DomainID 1. Continue?[y|n] :y
XSB#00-3 will be assigned to DomainID 1. Continue?[y|n] :y

XSCF> showdcl -v -d 1

DID   LSB   XSB   Status   No-Mem   No-IO    Float    Cfg-policy

01                Powered Off                         FRU
      00    00-1           False    False    False
      01    00-3           False    False    False
      02    -
      03    -
```

```
       04    -
       05    -
       06    -
       07    -
       08    -
       09    -
       10    -
       11    -
       12    -
       13    -
       14    -
       15    -

XSCF> poweron -d 1

DomainIDs to power on:1
Continue? [y|n] :y
01 :Powered on

XSCF> showboards -a

XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------- ---- ---- ---- ------- -------
00-0 00(00)   Assigned    y    y    n    Passed  Normal
00-1 01(00)   Assigned    y    y    n    Passed  Normal
00-2 00(01)   Assigned    y    y    n    Passed  Normal
00-3 01(01)   Assigned    y    y    n    Passed  Normal

XSCF> console -d 0
Connect to Domain#00?[y|n] :y

{0} ok
```

Domain Communication

Domain communication includes:

- Domain and Service Processor internal communication over the DSCP network
- Accessing a domain console from the Service Processor
- Logging in to a domain using an Ethernet connection

DSCP Network

The DSCP network establishes a link, using IP addresses, between the Service Processor and each domain. This link enables communication between the Service Processor and domains, and the secure transfer of information. Each domain must have its own IP address, and the Service Processor must have its own IP address.

DSCP is optimized to securely exchange control data such as error reports, fault events, and time synchronization, between each domain and the Service Processor.

Accessing a Domain Console from the Service Processor

You can log in to the Service Processor and use the `console` command to access a particular domain.

Once you have access to the domain console, you will get the standard Solaris console with associated prompts, based on the configured shell. You will be able to run all of the normal Solaris command-line interface commands. To run Solaris GUI-based commands, however, you must log in to the domain from a remote environment, not through the domain console.

Logging in Directly to a Domain

If your server is networked, you can log into a domain directly using standard Solaris applications, such as `telnet`, `rsh`, and `rlogin`. To ensure a secure connection, use `ssh`.

DVD Drive or Tape Drive Assignment

On a midrange server, the optional DVD drive or DAT drive can automatically be used by the domain on PSB/XSB 00-0.

On a high-end server, the DVD or DAT drives can be used by assigning them to a specific card port on an I/O unit. The devices are assigned to a specific port on an I/O unit using the `cfgdevice` command on the Service Processor, then connected using the `cfgadm` command on the Solaris OS. The DVD drives are read-only.

See "To Attach a DVD or Tape Drive While the Solaris OS Is Running (M8000/M9000 Servers)" on page 59 for instructions. You can also refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide* or to the `cfgadm`(1M) and `cfgdevice`(8) `man` pages for additional information.

Backup and Restore Operations

For domain backup and restore operations, refer to your backup software documentation for instructions. The Solaris OS documentation collection also contains information on backup and restore operations.

Dynamic Reconfiguration

Dynamic reconfiguration allows you to add or remove PSBs from system domains without stopping the Solaris OS. You can use dynamic reconfiguration to redistribute your system resources by adding or removing system boards as needed or to replace failed system boards with new ones. For more information, refer to the *Dynamic Reconfiguration User's Guide* and to the *Service Manual*.

XSCF Shell Procedures for Domain Configuration

This section describes these tasks:

- To Specify the XSB Mode
- To Set Up a Domain Component List
- To Assign an XSB to a Domain
- To Power On a Domain
- To Display System Board Status
- To Access a Domain From the XSCF Console

▼ To Specify the XSB Mode

1. **Log in to the XSCF console with** `platadm` **or** `fieldeng` **privileges.**
2. **Type the** `setupfru` **command:**

```
XSCF> setupfru -x mode sb location
```

where *mode* can be either 1 to specify a Uni-XSB or 4 to specify a Quad-XSB; `sb` is the system board device, and *location* is the location of the device, a number from 0-15.

3. **Verify the operation with the** `showfru` **command.**

▼ To Set Up a Domain Component List

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setdcl` **command:**

```
XSCF> setdcl -d domain_id -a lsb=xsb
```

   where *domain_id* is the domain you are setting the DCL for; *lsb* is the LSB number; and *xsb* is the XSB number.

3. **Verify the operation with the** `showdcl` **command.**

▼ To Assign an XSB to a Domain

1. **Log in to the XSCF console with** `platadm` **privileges or** `domainadm` **privileges for a specific domain.**
2. **Type the** `addboard` **command:**

```
XSCF> addboard -c assign -d domain_id xsb
```

   where *domain_id* is the domain to which the XSB is to be assigned; *xsb* is the XSB number to be assigned to the domain. For example, to assign XSB00-0 in domain 0, enter:

```
XSCF> addboard -c assign -d 0 00-0
```

   Once an XSB has been assigned to a domain, that XSB belongs to that domain until the domain unassigns it.

3. **Verify the operation with the** `showboards -a` **command.**

▼ To Power On a Domain

1. **Log in to the XSCF console with** `platadm` **or** `fieldeng` **privileges or** `domainadm` **or** `domainmgr` **privileges for a specific domain.**

2. **Type the** `poweron` **command:**

```
XSCF> poweron -d domain_id
```

where *domain_id* is the domain you want to power on. Only a user with `platadm` or `fieldeng` privileges can use the `-a` option to turn on power to all domains.

3. **Verify the domain is powered on by opening a console to it, with the** `console` **command.**

Refer to "To Access a Domain From the XSCF Console" on page 58.

▼ To Display System Board Status

1. **Log in to the XSCF console with** `platadm`, `platop`, **or** `fieldeng` **privileges or** `domainadm`, `domainmgr`, **or** `domainop` **privileges for a specific domain.**
2. **Type the** `showboards` **command:**

```
XSCF> showboards -a
```

▼ To Access a Domain From the XSCF Console

1. **Log in to the XSCF console with** `platadm`, `platop`, **or** `useradm` **privileges or** `domainadm`, `domainmgr`, **or** `domainop` **privileges for a specific domain.**
2. **Type the** `console` **command:**

```
XSCF> console -d domain_id
```

where *domain_id* is the domain you want to access. This command supports both interactive and read-only connections; the default is a read-write connection.

3. **To return to the XSCF console, press the Enter key, then the escape character, then type a period (.); by default the escape character is the pound sign (#):**

```
% #.
XSCF>
```

▼ To Attach a DVD or Tape Drive While the Solaris OS Is Running (M8000/M9000 Servers)

1. **If the Volume Management Daemon (`vold`) is running, stop the daemon:**

```
# /etc/init.d/volmgt stop
```

2. **Log in to the XSCF console with `platadm` privileges.**
3. **Type the `cfgdevice` command:**

   a. **To check the status of current drives:**

```
XSCF> cfgdevice -l
```

   b. **To attach a drive:**

```
XSCF> cfgdevice -c attach -p port_no
```

   where *port_no* is the port number in the specified domain where the device is to be attached. *port_no* is specified in the format: *IOU number-PCI slot numbe*r.

4. **Mount the drive by typing the `cfgadm` command:**

```
# cfgadm -c configure Ap_Id
```

   where *Ap_Id* is the attachment point of the controller, for example, `c0`.

5. **Restart the Volume Management Daemon (`vold`) if necessary:**

```
# /etc/init.d/volmgt start
```

▼ To Disconnect a DVD or Tape Drive While the Solaris OS Is Running (M8000/M9000 Servers)

1. **If the Volume Management Daemon (`vold`) is running, stop the daemon:**

```
# /etc/init.d/volmgt stop
```

2. **Detach the drive by typing the** `cfgadm` **command:**

```
# cfgadm -c unconfigure Ap_Id
```

where *Ap_Id* is the attachment point of the controller. For example, if the drive is connected to controller `c0`, you would type:

```
# cfgadm -c unconfigure c0::dsk/c0t4d0
# cfgadm -c unconfigure c0::rmt/0
```

3. **Log in to the XSCF console with** `platadm` **privileges.**

4. **Type the** `cfgdevice` **command:**

   a. **To check the status of current drives:**

```
XSCF> cfgdevice -l
```

   b. **To detach a drive:**

```
XSCF> cfgdevice -f -c detach -p port_no
```

where *port_no* is the port number in the specified domain where the device is to be detached. *port_no* is specified in the format: *IOU number-PCI slot numbe*r.

5. **Restart the Volume Management Daemon (**`vold`**) if necessary:**

```
# /etc/init.d/volmgt start
```

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages	`setupfru`(8), `showfru`(8), `setdcl`(8), `showdcl`(8), `addboard`(8), `moveboard`(8), `deleteboard`(8), `showboards`(8), `xntpd`(1M), `showdevices`(8), `showconsolepath`(8), `console`(8), `sendbreak`(8), `poweron`(8), `poweroff`(8), `reset`(8), `cfgdevice`(8), `cfgadm`(1M), `setdomainmode`(8)
Solaris OS documentation collection	Solaris OS installation; NTP; domains; backup operations
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	Domains
Dynamic Reconfiguration User's Guide	Domains
Service Manual	Physical component removal; FRUs

CHAPTER 5

Audit Configuration

A SPARC Enterprise M*x*000 server can have multiple domains. Those domains must be as secure as if they were running on physically separate servers. To help ensure that level of security, XSCF firmware provides the audit measures described in this chapter.

This chapter contains these sections:

- About Auditing
- XSCF Shell Procedures for Auditing
- Related Information

About Auditing

A SPARC Enterprise M*x*000 server logs all Service Processor events that could be relevant to security, such as system startup and shutdown, user login and logout, and privilege changes.

An audit record contains information about a single event, what caused it, the time it occurred, and other relevant information. A collection of audit records that are linked is called an audit *trail*. An audit trail can reveal suspicious or abnormal patterns of system behavior, in addition to identifying which user was responsible for a particular event.

Auditing is implemented through:

- Audit Records
- Audit Events
- Audit Classes
- Audit Policy
- Audit File Tools

Audit Records

Audit records are stored in audit files on a 4-megabyte file system on the Service Processor. You cannot change the size reserved for the audit files, but you can transfer the files manually to remote storage at any time. You can also configure auditing for automatic transfers.

Audit files are stored in binary format, although you can export them to XML.

The audit file system switches storage between two partitions. Audit records are stored in one partition until it becomes full, then new records are stored in the other partition. Records in a full partition can be moved to a remote location, according to the audit policy.

If audit policy or network problems impede remote storage, the system generates an alarm. You can clear space by manually transferring the files to remote storage or by deleting them. Until you clear space, new records are dropped.

Because local space is limited to 4 megabytes, the partitions fill up quickly. If you do not configure audit policy to automatically transfer files to remote storage, you will have to intervene frequently or begin to drop records. If you are unable to maintain consistent audit trails, the utility of the audit system is limited. Typically, you either set up sufficient remote space and automatic transfers or disable the audit capability.

Audit Events

Audit events are:

- Changes to the Service Processor configuration, for example, an IP address change
- Any request to perform an operation on an object protected by the access control policy
- All use of authentication
- Tests of password strength, for example, tests done by the `password` command to check whether a password contains enough nonalphabetical characters
- Modifications to the access control attributes associated with an object, for example, changes to controls on which domains a board might be in
- Changes made to user security attributes, for example, password or privileges
- Reading information from the audit records (including unsuccessful attempts)
- Modifications to the audit policy
- Actions taken due to the exceeding of a audit trail size threshold
- Actions taken due to audit storage failure
- Modifications made by administrators to the audit trail

- Changes to the time

The minimum data recorded for each event includes:

- Date and time of the event
- Type of event
- Who caused the event
- Outcome of the event (success or failure)

Audit Classes

Audit classes are categories for grouping and sorting audit events. The SPARC Enterprise M*x*000 server provides a predefined set of audit classes, for example, log-in events and service-related events. You cannot define additional audit classes or change the events in a class. Refer to the `setaudit`(8) `man` page for a list of audit classes.

Audit Policy

Audit policy determines how the auditing feature is implemented at your site. You can configure the following aspects of auditing:

- Whether it is enabled or disabled
- Types of event that are audited
- Which users have their events audited
- Remote directories for storing audit records
- Threshold of local capacity at which a warning is issued
- Action when both audit partitions are full

The default audit policy is as follows:

- Auditing is enabled
- Records are dropped and counted when the audit trail is full
- All events are enabled for auditing
- Global user audit policy is set to enabled
- Per-user audit policy for all users is set to `default` (that is, enabled)
- Audit warning thresholds are set at 80 percent and 100 percent full
- Email warnings are disabled

Audit File Tools

You can manage audit files from the Service Processor, using a tool for viewing audit files. Refer to the `viewaudit`(8) `man` page for details on this tool.

XSCF Shell Procedures for Auditing

This section describes these tasks:

- To Enable or Disable Writing of Audit Records to the Audit Trail
- To Configure an Auditing Policy
- To Display Whether Auditing is Enabled Or Disabled
- To Display Current Auditing Policy, Classes, or Events

▼ To Enable or Disable Writing of Audit Records to the Audit Trail

1. **Log in to the XSCF console with** `auditadm` **privileges.**
2. **Type the** `setaudit` **command:**

```
XSCF> setaudit enable|disable
```

where `enable` enables writing of audit records, and `disable` disables writing of audit records.

▼ To Configure an Auditing Policy

1. **Log in to the XSCF console with** `auditadm` **privileges.**
2. **Type the** `setaudit` **command:**

```
XSCF> setaudit [-p count|suspend] [-m mailaddr] [-a users=
enable|disable|default] [-c classes={enable|disable}] [-e events=
enable|disable] [-g {enable|disable}] [-t percents]
```

Refer to the `setaudit`(8) `man` page for details on option information.

3. **Verify the operation with the** `showaudit all` **command:**

```
XSCF> showaudit all
```

▼ To Display Whether Auditing is Enabled Or Disabled

1. **Log in to the XSCF console with** `auditadm` **privileges.**
2. **Type the** `showaudit` **command:**

```
XSCF> showaudit
Auditing: enabled
```

▼ To Display Current Auditing Policy, Classes, or Events

1. **Log in to the XSCF console with** `auditadm` **privileges.**
2. **Type the** `showaudit all` **command:**

```
XSCF> showaudit all
```

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages	`setaudit`(8), `showaudit`(8), `viewaudit`(8)
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	Audit administration

CHAPTER 6

Log Archiving Facility

You can set up the Service Processor to automatically archive its log data on a remote host.

This chapter contains these sections:

- About Log Archiving
- Solaris OS Procedures for Log Archiving
- XSCF Shell Procedures for Log Archiving
- Related Information

About Log Archiving

The persistent storage space on a Service Processor is limited. A portion of this space is set aside for logs, such as audit logs and error logs. Due to the limited space, some logs can grow to the point where old log entries must be overwritten or deleted.

These sections provide details on log archiving:

- Using the Log Archiving Facility
- Archive Host Requirements
- Log Archiving Errors
- Using the `snapshot` Tool

Using the Log Archiving Facility

Log archiving increases the storage space available for logs on the Service Processor by transferring and storing log data on a server known as the *archive host*.

All connections established through log archiving are encrypted. The log archiving feature provides the ability to use an RSA public key to authenticate the archive host. You manage this public key on the Service Processor.

By default, log archiving is disabled. To use log archiving, you set up an archive host, and then enable log archiving on the Service Processor.

When enabled, log archiving periodically uses the secure copy program (`scp`) to transfer new log data to the archive host. Log archiving uses `ssh` to monitor the disk space consumed by archives. It deletes old archives when necessary, so that the space consumed by the archives will never exceed user-configurable archive space limits. However, for security reasons, log archiving does not automatically delete audit log archives. You can manually delete audit log archives that are no longer needed.

FIGURE 6-1 illustrates how log archiving works.

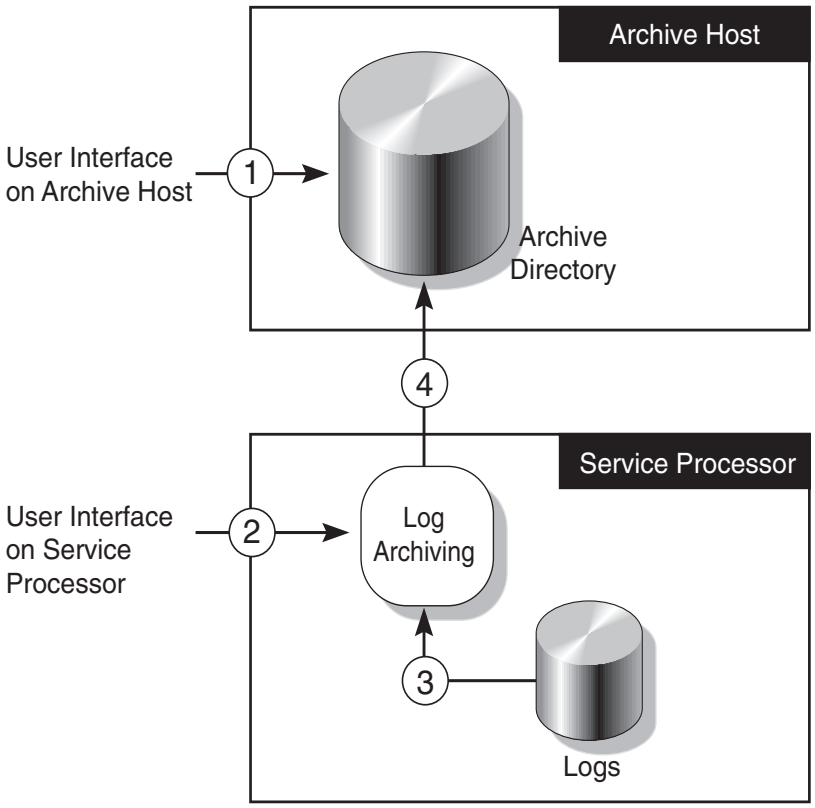

FIGURE 6-1 Log Archiving

As shown in FIGURE 6-1,

(1) Before enabling log archiving, create an archive directory on the archive host. There should be a separate archive directory for each system that uses the archive host. The directory permissions should be set so that only authorized users can access its contents.

(2) You configure the log archiving feature.

(3) As new data accumulates in logs, log archiving polls log files at fixed intervals to determine when new data needs to be archived.

(4) Log archiving uses `scp` to transfer log data to the archive host. It uses `ssh` to manage the logs which it previously copied.

Archive Host Requirements

As the Service Processor keeps track of archive space on the archive host, you should not store other files in these archive directories.

It is possible to set up the Service Processor so that it uses one of the domains in the same system as an archive host. However, this configuration does not provide optimal reliability and serviceability. Typically, a separate, remote server functions as the archive host.

Log Archiving Errors

The log archiving system handles typical errors by retrying and recording errors in the Event Log. Possible error causes include archive host downtime, network outages, and misconfiguration of the Service Processor and/or the archive host. You can use the `showarchiving` command to view the details of the last ten archiving failures, including the first 1000 characters of output from any command that failed.

Using the `snapshot` Tool

Log data can also be collected and transferred from the Service Processor with the `snapshot` command. The `snapshot` tool does not extend or replace any other functionality, such as log archiving or logging of information using `syslog`. Refer to the `snapshot`(8) `man` page for details on this tool.

Solaris OS Procedures for Log Archiving

▼ To Configure the Log Archive Host

1. **Select a user account on the server that will be used as the archive host that the Service Processor will use to log in.**
2. **Log in to the archive host and create an archive directory.**
3. **Set the permissions of the archive directory as desired. The Service Processor log-in account must have read, write, and execute (`rwx`) permissions.**

XSCF Shell Procedures for Log Archiving

This section describes these tasks:

- To Enable Log Archiving
- To Disable Log Archiving
- To Display Log Archiving Configuration and Status
- To Display Log Archiving Error Details

▼ To Enable Log Archiving

1. **Log in to the XSCF console with `platadm` privileges.**
2. **Type the `setarchiving` command:**

```
XSCF> setarchiving -t user@host:directory -r
```

where *user@host:directory* is the user name, log archive host, and directory where the logs are to be stored, and `-r` prompts for the password for `ssh` login. Refer to the `setarchiving` `man` page for additional options.

3. **Type the** `setarchiving enable` **command:**

```
XSCF> setarchiving enable
```

After tests indicate the archive host is set up correctly, log archiving is enabled effective immediately. If the tests fail, you receive an error message that log archiving was not enabled, and the reason why.

▼ To Disable Log Archiving

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setarchiving` **command:**

```
XSCF> setarchiving disable
```

▼ To Display Log Archiving Configuration and Status

1. **Log in to the XSCF console with** `platadm`**,** `platop`**, or** `fieldeng` **privileges.**
2. **Type the** `showarchiving` **command:**

```
XSCF> showarchiving
```

▼ To Display Log Archiving Error Details

1. **Log in to the XSCF console with** `platadm`**,** `platop`**, or** `fieldeng` **privileges.**
2. **Type the** `showarchiving` **command:**

```
XSCF> showarchiving -e
```

The details of the last ten archiving failures will be displayed.

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages	`setarchiving`(8), `showarchiving`(8), `showlogs`(8), `snapshot`(8)
SPARC Enterprise M4000/M5000/M8000/M9000 Servers XSCF User's Guide	Logs; saving logs to a USB device

CHAPTER 7

Capacity on Demand

This chapter describes how to manage system resources with the Capacity on Demand (COD) feature of your server.

This chapter contains these sections:

- About Capacity on Demand
- XSCF Shell Procedures for Using COD
- Related Information

For information on ordering and purchasing COD licenses, refer to the *COD User's Guide* for your server.

About Capacity on Demand

Capacity on Demand is an option that allows you to purchase spare processing resources (CPUs) for your server. The spare resources are provided in the form of one or more CPUs on COD boards that are installed on your server. However, to access these COD CPUs, you must first purchase the COD right-to-use (RTU) licenses for them. Under certain conditions, you can use COD boards before actually purchasing a license.

These sections provide details:

- COD Boards
- COD License Purchase
- License Installation
- License Allocation
- Headroom Management
- License Violations

COD Boards

A COD board is a system board that has been configured at the factory for COD capability. COD boards come in the same configurations as standard system boards. The number of CPUs per COD board depends on the SPARC Enterprise M*x*000 server configuration that you purchased.

COD boards are subject to the same limitations for mixed architectures and CPU speeds as system boards. Likewise, COD board software requirements, such as the Solaris OS or OpenBoot PROM version, are the same as those of system boards. A SPARC Enterprise M*x*000 server can have any combination of COD and system boards. It can even be configured entirely with COD boards.

Once a COD board has been licensed, you can configure it into domains in the same way as a system board. Until it has been licensed, however, you cannot configure it into a domain.

COD boards are identified by a special field-replaceable unit (FRU) ID and by a COD label. Except for their FRU ID, label, and COD capability, once COD boards are licensed, they are handled by the rest of the hardware and software in exactly the same way as system boards. COD boards fully support dynamic reconfiguration operations.

You can order COD boards either when you order your server, in which case they arrive already installed, or as an option. The SPARC Enterprise M4000 and M5000 servers can not add option COD boards after shipment from the factory; COD capability for these two servers must be ordered with the server.

For more information about COD boards and replacing COD boards (field-replaceable units, or FRUs) in your server, see the *COD User's Guide* and the *Service Manual.*

COD License Purchase

The purchase of a COD RTU license entitles you to receive a license *key*, which enables the appropriate number of COD processors. A license key can grant access to multiple RTUs.

A COD license is assigned to a specific server, one license per processor (CPU). All the licenses assigned to a server are handled as a floating pool of licenses for all the COD processors installed on that server. For example, if you have a server with two COD boards with four processors each, but you will only use six of those processors, all you need is six licenses. Those six licenses can be used by all eight processors, but only six at a time.

At least 50 license keys can be installed on a SPARC Enterprise M*x*000 server. A COD license has no expiration date.

Although a COD license can be used by any COD processor, it cannot be moved from one server to another. A COD license is limited to the processors on a specific server. If those processors are moved to another server, the license becomes invalid.

License Installation

A license key is comprised of text lines, which can be added to the COD license database. A single license key can grant access to multiple RTUs, as specified when the key is generated.

After you purchase a license, you must install the license keys in the COD license database. The license database is stored in nonvolatile memory on the Service Processor. In a system with more than one Service Processor, failover of the COD license database is supported. COD locks its license keys to the individual Chassis HostID of the system.

In case the license database is lost or corrupted, make sure you keep copies of your licenses and license keys.

License Allocation

The software allocates COD licenses automatically on a first-come, first-served basis. However, you can reserve licenses if you want to make sure a specific number of COD licenses are allocated to a particular domain.

Licenses are allocated to COD resources either when a domain with a COD board is powered on or when a new COD board is installed and powered on.

At board power on, the Service Processor determines which processing resources are in working order and requests licenses for them. The COD software checks its license database and current usage, determines which boards are COD boards, and allocates licenses to their resources. It then tells the Service Processor which resources to configure into the domain.

The Service Processor configures only the COD resources approved by the COD licensing software. Any COD resource that remains unlicensed is not configured into the domain and is assigned a `COD-disabled` status.

When you remove a COD board from a domain through a reconfiguration operation, when a domain containing a COD board is shut down normally, or when the Service Processor detects a fault and unconfigures a board from the domain, the COD licenses for the resources on those boards are released and added to the pool of available licenses.

License allocation does not change during a Service Processor reboot or failover. All licenses remain allocated to their resources.

You can reserve COD licenses for specific domains by using the `setcod` command. After power on, reserved licenses are first allocated to their domains, and then remaining licenses are allocated on a first-come, first-served basis to the remaining resources. When a domain is powered off, the reverse happens: first the unreserved licenses are released to the pool, then the reserved licenses are released.

For example, assume your server had 10 COD licenses and you reserved them for these domains:

```
PROC RTUs reserved for domain 0: 4
PROC RTUs reserved for domain 1: 2
PROC RTUs reserved for domain 2: 0
PROC RTUs reserved for domain 3: 0
```

When the domains were first powered on, four licenses would be assigned to domain 0 and two licenses to domain 1. The remaining four licenses would be available on a first-come, first-served basis to all four domains (0, 1, 2, and 3).

Headroom Management

Headroom is the capability to use up to four COD processors per server before actually purchasing a license. Headroom allows you to activate a COD board under these conditions:

- As a hot spare to replace a failed system board
- When you intend to purchase a license but need to use the resources immediately

---

Note – Once you have used headroom to activate a COD resource, you are contractually obligated to purchase a license for it.

By default, COD resources arrive with headroom disabled. You can use the `setcod` command to establish it. However, if all your COD resources are already licensed, configuring headroom will have no effect. In that case, you need to install additional COD boards to retain your headroom capacity. You can also reduce or disable headroom at any time.

While headroom is in use, warning messages appear on the console every four hours. Once you either deactivate the hot-spared COD board or purchase a license for the resources and enter the license keys, the warning messages stop. When a license key is added, the headroom is automatically reduced by the quantity provided by the license key.

License Violations

A license violation occurs if more resources are in use than are currently licensed on the server. These events can cause a license violation:

- The license database is lost or corrupted while the system is running. This state is detected on the subsequent reboot.

  This situation can be remedied by reentering the missing license keys, using the `addcodlicense` command.

- You delete COD licenses with the force option (`deletecodlicense -f`) while the server is still using those licenses.

  This could be a valid action in certain cases. For example, you might want to delete unwanted COD licenses, but want to delay shutting down the domain.

- You disable headroom while the server is still using those resources.

Once the system detects a license violation, the Service Processor will post a notice on the server console and ensure that no additional COD resources are brought online until the violation is corrected. In the meantime, it will not shut down domains or COD resources.

XSCF Shell Procedures for Using COD

This section describes these tasks:

- To Install a COD License
- To Delete a COD License
- To Reserve Licenses for Allocation
- To Increase or Decrease Headroom
- To Disable Headroom
- To Display COD Information
- To Display COD License Status
- To Display Usage Statistics for COD Resources

▼ To Install a COD License

This procedure installs a COD license and, if headroom is enabled, decreases headroom to compensate for each new license. This automatic reduction in headroom is designed to avoid accidental abuse of headroom. You can increase headroom again manually after installing the COD license. See "To Increase or Decrease Headroom" on page 82.

1. **Log in to the XSCF console with** `platadm` **privileges.**

2. **Type the** `addcodlicense` **command:**

```
XSCF> addcodlicense license-signature
```

where *license-signature* is the complete COD license key. For example:

```
XSCF> addcodlicense \
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxx
```

3. **Verify that the license key was added to the license database by typing the** `showcodlicense -r` **command.**

The COD RTU license key that you added should be listed in the `showcodlicense` output. See "To Display COD License Status" on page 84.

▼ To Delete a COD License

Before deleting a license, the COD software determines whether sufficient licenses are available from the pool of installed licenses plus headroom. If all licenses are in use and no headroom is available, the operation will fail. You can force the operation by using the `-f` option in Step 3, but doing so will overcommit any license reservations that might be in effect.

1. **Log in to the XSCF console with** `platadm` **privileges.**

2. **Verify that you have enough licenses or headroom to cover COD resources currently in use.**

Use the `showcodlicense` command, as described in "To Display COD License Status" on page 84. If you do not have sufficient licenses or headroom to compensate, power off one or more domains or disconnect the appropriate number of boards.

3. **Type the** `deletecodlicense` **command:**

```
XSCF> deletecodlicense license-signature
```

where *license-signature* is the complete COD license key.

4. **Verify that the license key was removed from the license database by typing the `showcodlicense -r` command.**

   The COD RTU license key that you deleted should not be listed in the `showcodlicense` output. See "To Display COD License Status" on page 84.

▼ To Reserve Licenses for Allocation

You need to reserve licenses only if you want to make sure a specific number of COD licenses are allocated to a particular domain.

1. **Log in to the XSCF console with `platadm` privileges.**
2. **Type the `setcod` command.**

   You can use one of two methods, as follows.

   - Use `setcod` command with the `-d` *domain_id* and the *license_quantity* options:

```
XSCF> setcod -d domain_id license_quantity
```

   For example:

```
XSCF> setcod -d 1 4
```

   - Use the `setcod` command with no options.

     This option allows you to reserve licenses for all domains at once. First, the number of available licenses (8 in the example below) and the headroom quantity prompt are displayed:

```
XSCF> setcod
COD
---
PROC RTUs installed: 8
PROC Headroom Quantity (0 to disable, 4 MAX) [0]:
```

   a. **Enter a headroom number or press Return to leave the headroom unchanged.**

The following prompts are displayed, in order:

```
PROC RTUs reserved for domain 0 (6 MAX) [0]:
PROC RTUs reserved for domain 1 (6 MAX) [2]:
PROC RTUs reserved for domain 2 (4 MAX) [0]:
PROC RTUs reserved for domain 3 (4 MAX) [0]:
```

b. Enter the number of licenses reserved for each domain.

The currently reserved number appear in parentheses. Do not exceed the number of available licenses. To leave a reservation unchanged, press Return.

3. Verify the allocation with the `showcod` command.

▼ To Increase or Decrease Headroom

1. Log in to the XSCF console with `platadm` privileges.

2. Type the `setcod` command.

You can use one of two methods, as follows.

- Use `setcod` command with the *headroom* option:

```
XSCF> setcod headroom
```

where *headroom* can be a number from 1 to 4. For example:

```
XSCF> setcod 4
```

- Use the `setcod` command with no options.

If you are not sure of the headroom that is available, enter the `setcod` command with no options; the output displays the number of available licenses and the current headroom quantity (a number from 0 to 4).

```
XSCF> setcod
COD
---
PROC RTUs installed: 8
PROC Headroom Quantity (0 to disable, 4 MAX) [0]:
```

You are prompted to enter the *headroom* number. Press Return when finished.

3. **Verify the headroom quantity is correct by typing the** `showcod` **command.**

   For example, if you entered 4 as the headroom number, the output would be similar to:

```
XSCF> showcod
Chassis HostID: 80d88800
PROC RTUs installed: 8
PROC Headroom Quantity: 4
...
```

▼ To Disable Headroom

1. **Log in to the XSCF console with** `platadm` **privileges.**
2. **Type the** `setcod` **command and a headroom number of zero:**

```
XSCF> setcod 0
```

3. **Verify that the headroom is disabled by typing the** `showcod` **command.**

   For example:

```
XSCF> setcod 0

XSCF> showcod
Chassis HostID: 80d88800
PROC RTUs installed: 8
PROC Headroom Quantity: 0
...
```

▼ To Display COD Information

1. **Log in to the XSCF console with** `platadm`**,** `platop`**,** `domainadm`**, or** `domainop` **privileges, or** `domainmgr` **privileges for a specific domain.**

2. **Type the** `showcod` **command.**

   The output displays the server's Chassis HostID, number of licenses (`PROC RTUs installed`), headroom quantity, and number of licenses reserved for each domain. For example:

```
XSCF> showcod
Chassis HostID: 80e3e446
PROC RTUs installed: 10
PROC Headroom Quantity: 0
PROC RTUs reserved for domain 0: 4
PROC RTUs reserved for domain 1: 0
PROC RTUs reserved for domain 2: 0
PROC RTUs reserved for domain 3: 0
```

   To display COD information only for a specific domain, use the `showcod -d` *domain_id* command, where *domain_id* can be 0-23 depending on system configuration.

▼ To Display COD License Status

1. **Log in to the XSCF console with** `platadm` **or** `platop` **privileges.**

2. **Type the** `showcodlicense` **command.**

   The output displays the resource description, license version number, expiration date, number of licenses, and license status. For example:

```
XSCF> showcodlicense

Description  Ver   Expiration  Count  Status
-----------  ---   ----------  -----  ------
PROC          01         NONE      8  GOOD
```

   To display license information in raw key format, use the `-r` option. For example:

```
XSCF> showcodlicense -r

01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxx
```

   To display license information in verbose mode, use the `-v` option. For example:

```
XSCF> showcodlicense -v

Description  Ver   Expiration  Count  Status
-----------  ---   ----------  -----  ------
PROC          01         NONE      1  GOOD
01:84000000:000000001:0301010100:1:00000000:xxxxxxxxxxxxxxxxxxxxx
PROC          01         NONE      2  GOOD
01:84000000:000000004:0301010100:2:00000000:xxxxxxxxxxxxxxxxxxxxx
```

▼ To Display Usage Statistics for COD Resources

1. **Log in to the XSCF console with** `platadm` **or** `platop` **privileges, or** `domainadm`**,** `domainop`**, or** `domainmgr` **privileges for a specific domain.**

2. **Type the** `showcodusage` **command.**

   The output displays a summary of license usage by resource type and for each domain. For example:

```
XSCF> showcodusage

Resource      In Use  Installed  Licensed  Status
--------      ------  ---------  --------  ------
PROC               0          4         0  OK: 0 available
Domain/Resource  In Use  Installed  Reserved
---------------  ------  ---------  --------
0  - PROC             0          4         0
1  - PROC             0          0         0
2  - PROC             0          0         0
3  - PROC             0          0         0
Unused - PROC         0          0         0
```

   To display usage statistics only for domains or resources, use the `showcodusage -p domain` command or the `showcodusage -p resource` command. All COD usage information can be displayed with the `showcodusage -p all` command.

   You can also use the `showboards` command to identify which board is a COD board. The output from this command has a column titled “COD”. This column contains an “n” for a non-COD board or a “y” for a COD board. For example:

```
XSCF> showboards -v -a

XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   SP       Unavailable n    n    n    Unknown Normal   n
01-0   SP       Unavailable n    n    n    Fail    Failed   n
```

Related Information

For additional information on this chapter's topics, see:

Resource	Information
`man` pages	`setcod`(8), `showboards`(8), `showcodusage`(8), `showcodlicense`(8), `showcod`(8), `addcodlicense`(8), `deletecodlicense`(8)
COD User's Guide	Ordering COD licenses; additional COD procedures
Service Manual	Physical component removal; FRUs

APPENDIX **A**

Mapping Device Path Names

This appendix describes how to map device path names to physical system devices. It contains these sections:

- Device Mapping and Logical System Board Numbers
- CPU Mapping
- I/O Device Mapping

Device Mapping and Logical System Board Numbers

The physical address represents a physical characteristic that is unique to the device. Examples of physical addresses include the bus address and the slot number. The slot number indicates where the device is installed.

The logical system board (LSB) number affects both the processor numbering and the I/O device paths in the SPARC Enterprise M*x*000 server. Physical resources are assigned to LSBs in the specified domain using the `setdcl` command. It is the LSB numbers that the Solaris OS uses.

CPU Mapping

Each LSB has a bank of 32 processor numbers assigned to it. Each processor has two cores, and each core has two strands.

An LSB has four processors as a maximum (when a Uni-XSB is assigned to the LSB); therefore, an LSB needs 16 processor IDs. Note that 32 IDs are assigned for future expansion.

TABLE A-1 shows the relationship between LSB numbers and starting processor ("proc") numbers, in hexidecimal/decimal format. The Solaris `prtdiag` command provides the LSB numbers and CPU chip numbers in decimal format for components that are part of the domain.

TABLE A-1 LSB Numbers and Starting Processor Numbers

LSB Number	CPU Chip 0	CPU Chip 1	CPU Chip 2	CPU Chip 3
00	00/00	08/08	10/16	18/24
01	20/32	28/40	30/48	38/56
02	40/64	48/72	50/80	58/88
03	60/96	68/104	70/112	78/120
04	80/128	88/136	90/144	98/152
05	a0/160	a8/168	b0/176	b8/184
06	c0/192	c8/200	d0/208	d8/216
07	e0/224	e8/232	f0/240	f8/248
08	100/256	108/264	110/272	118/280
09	120/288	128/296	130/304	138/312
10	140/320	148/328	150/336	158/344
11	160/352	168/360	170/368	178/376
12	180/384	188/392	190/400	198/408
13	1a0/416	1a8/424	1b0/432	1b8/440
14	1c0/448	1c8/456	1d0/464	1d8/472
15	1e0/480	1e8/488	1f0/496	1f8/504

CPU Numbering Examples

This section contains examples of CPU numbering, using the output of the `showboards` command on the Service Processor, and the output of the `prtdiag` command on a domain.

```
XSCF> showboards -a

XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------- ---- ---- ---- ------- --------
00-0 00(00)   Assigned    y    y    y    Passed  Normal
00-1 00(01)   Assigned    y    y    y    Passed  Normal
00-2 00(04)   Assigned    y    y    y    Passed  Normal
00-3 00(05)   Assigned    y    n    n    Passed  Normal
01-0 01(00)   Assigned    y    y    y    Passed  Normal
01-1 01(09)   Assigned    y    y    y    Passed  Normal
01-2 01(06)   Assigned    y    n    n    Passed  Normal
01-3 01(07)   Assigned    y    n    n    Passed  Normal
```

```
domain_0# prtdiag -v
...
================================== CPUs ==================================

       CPU              CPU            Run       L2$       CPU       CPU
LSB    Chip              ID            MHz        MB       Impl.     Mask
---    ----      --------------------  ----      ---       -----     ----
 00      0           0,   1,   2,   3   2150      4.0          6      129
 01      1          40,  41,  42,  43   2150      4.0          6      129
 04      2         144, 145, 146, 147   2150      4.0          6      129
 05      3         184, 185, 186, 187   2150      4.0          6      129

==========================================================================
```

```
domain_1# prtdiag -v
...
================================== CPUs ==================================

       CPU              CPU            Run       L2$       CPU       CPU
LSB    Chip              ID            MHz        MB       Impl.     Mask
---    ----      --------------------  ----      ---       -----     ----
 00      0           0,   1,   2,   3   2150      4.0          6      129
 09      1         296, 297, 298, 299   2150      4.0          6      129
 06      2         208, 209, 210, 211   2150      4.0          6      129
 07      3         248, 249, 250, 251   2150      4.0          6      129

==========================================================================
```

I/O Device Mapping

I/O device paths are dictated by which LSB the I/O unit is assigned to.

The M4000 and M5000 servers have only one I/O controller on the I/O unit (IOU). For an XSB in Uni-XSB mode, all I/O is on XSB#*xx*-0. For an XSB in Quad-XSB mode, internal resources, the PCI-X slot, and two PCIe slots are on XSB#*xx*-0, and two PCIe slots are on XSB#*xx*-1.

The M8000 and M9000 servers have two I/O controllers; therefore, each XSB can have two PCIe slots assigned to it.

TABLE A-2 shows the LSB numbers and the corresponding device path values that are used in I/O device mapping on the SPARC Enterprise M*x*000 server.

TABLE A-2 LSB Numbers and Device Path Values

LSB Number	Device Path Value
00	No value
01	1
02	2
03	3
04	4
05	5
06	6
07	7
08	8
09	9
10	a
11	b
12	c
13	d
14	e
15	f

I/O Device Mapping on the M4000 and M5000 Servers

TABLE A-3 shows the device mapping on a midrange server. In the device path, *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2.

TABLE A-3 I/O Device Mapping on a Midrange Server

Slot	Host Bus Adapter Slot Type	OpenBoot PROM Device Path
IOU Slot 0	PCI-X	/pci@*x*0,600000/pci@0/pci@8/pci@0,1
IOU Slot 1	PCIe	/pci@*x*0,600000/pci@0/pci@9
IOU Slot 2	PCIe	/pci@*x*1,700000
IOU Slot 3	PCIe	/pci@*x*2,600000
IOU Slot 4	PCIe	/pci@*x*3,700000

Internal Devices on the M4000 and M5000 Servers

The internal M4000/M5000 devices, which are located at the XSB location 00-0 or 01-0 (regardless of Uni-XSB or Quad-XSB mode), are shown in TABLE A-4 and TABLE A-5. In the device path, *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2.

TABLE A-4 Internal Devices and Device Paths on the M4000 and M5000 Servers

XSB 00-0/IOU 0 Accessible Internal Devices (M4000/M5000)	Device Physical Location	OpenBoot PROM Device Path
Network Port 0	IOU	/pci@*x*0,600000/pci@0/pci@8/pci@0/network@2
Network Port 1	IOU	/pci@*x*0,600000/pci@0/pci@8/pci@0/network@2,1
HD0	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/disk@0
HD1	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/disk@1
CD/DVD	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/disk@3
DAT	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/tape@2

TABLE A-5 Internal Devices and Device Paths on the M5000 Server

XSB 01-0/IOU 1 Accessible Internal Device (M5000)	Device Physical Location	OpenBoot PROM Device Path
Network Port 0	IOU	/pci@*x*0,600000/pci@0/pci@8/pci@0/network@2
Network Port 1	IOU	/pci@*x*0,600000/pci@0/pci@8/pci@0/network@2,1
HD2	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/disk@0
HD3	System	/pci@*x*0,600000/pci@0/pci@8/pci@0/scsi@1/disk@1

I/O Device Mapping on the M8000 and M9000 Servers

TABLE A-6 shows the device mapping on a high-end server. In the PCIe device path, *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2. *xx* is the XSB number and is in the range from 00-15.

TABLE A-6 I/O Device Mapping on a High-end Server

PCIe Slot	Uni-XSB*	Quad-XSB†	OpenBoot PROM PCIe Device Path‡
IOU Slot 0	*xx*-0	*xx*-0	pci@*x*0,600000
IOU Slot 1	*xx*-0	*xx*-0	pci@*x*1,700000
IOU Slot 2	*xx*-0	*xx*-1	pci@*x*2,600000
IOU Slot 3	*xx*-0	*xx*-1	pci@*x*3,700000
IOU Slot 4	*xx*-0	*xx*-2	pci@*x*4,600000
IOU Slot 5	*xx*-0	*xx*-2	pci@*x*5,700000
IOU Slot 6	*xx*-0	*xx*-3	pci@*x*6,600000
IOU Slot 7	*xx*-0	*xx*-3	pci@*x*7,700000

* *xx* is the XSB number, in the range of 00-15.

† *xx* is the XSB number, in the range of 00-15.

‡ *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2.

Internal Devices on the M8000 and M9000 Servers

The IOUA is a PCIe Host Bus Adapter that provides access to internal devices when installed at specific locations. The IOUA contains two 1Gb Ethernet ports on the card ("on-board"). When the IOUA is installed at specific locations, it also provides access to storage located on the IOU, as well as platform DVD/DAT resources at the locations shown in TABLE A-7. In the PCIe device path, *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2. *xx* is the XSB number and is in the range from 00-15. *nn* is the number associated with the PSB to which the DVD or DAT device is attached, as further explained in the table footnote.

TABLE A-7 Internal Devices and Device Paths on a High-end Server

PCIe Slot	Uni-XSB*	Quad-XSB†	OpenBoot PROM PCIe Device Path‡	OpenBoot PROM IOUA HBA On-board, IOU, and Platform Accessible Devices§
IOU Slot 0	*xx*-0	*xx*-0	pci@*x*0,600000	.../pci@0,1/network@1 (IOUA HBA On-board BGE Port 0) .../pci@0,1/network@1,1 (IOUA HBA On-board BGE Port 1) .../pci@0/scsi@1/disk@0 (IOU HD0; SCSI Target 0) .../pci@0/scsi@1/disk@1 (IOU HD1; SCSI Target 1) .../pci@0/scsi@1/disk@4 (Platform CD/DVD at cfgdevice port *nn*-0; SCSI Target 4) .../pci@0/scsi@1/tape@5 (Platform DAT at cfgdevice port *nn*-0; SCSI Target 5)
IOU Slot 1	*xx*-0	*xx*-0	pci@*x*1,700000	
IOU Slot 2	*xx*-0	*xx*-1	pci@*x*2,600000	.../pci@0,1/network@1 (IOUA HBA On-board BGE Port 0) .../pci@0,1/network@1,1 (IOUA HBA On-board BGE Port 1) .../pci@0/scsi@1/disk@4 (Platform CD/DVD at cfgdevice port *nn*-2; SCSI Target 4) .../pci@0/scsi@1/tape@5 (Platform DAT at cfgdevice port *nn*-2; SCSI Target 5)
IOU Slot 3	*xx*-0	*xx*-1	pci@*x*3,700000	.
IOU Slot 4	*xx*-0	*xx*-2	pci@*x*4,600000	.../pci@0,1/network@1 (IOUA HBA On-board BGE Port 0) .../pci@0,1/network@1,1 (IOUA HBA On-board BGE Port 1) .../pci@0/scsi@1/disk@0 (IOU HD2; SCSI Target 0) .../pci@0/scsi@1/disk@1 (IOU HD3; SCSI Target 1) .../pci@0/scsi@1/disk@4 (Platform CD/DVD at cfgdevice port *nn*-4; SCSI Target 4) .../pci@0/scsi@1/tape@5 (Platform DAT at cfgdevice port *nn*-4; SCSI Target 5)

TABLE A-7 Internal Devices and Device Paths on a High-end Server *(Continued)*

PCIe Slot	Uni-XSB*	Quad-XSB†	OpenBoot PROM PCIe Device Path‡	OpenBoot PROM IOUA HBA On-board, IOU, and Platform Accessible Devices§
IOU Slot 5	*xx*-0	*xx*-2	pci@*x*5,700000	
IOU Slot 6	*xx*-0	*xx*-3	pci@*x*6,600000	.../pci@0,1/network@1 (IOUA HBA On-board BGE Port 0) .../pci@0,1/network@1,1 (IOUA HBA On-board BGE Port 1) .../pci@0/scsi@1/disk@4 (Platform CD/DVD at cfgdevice port *nn*-6; SCSI Target 4) .../pci@0/scsi@1/tape@5 (Platform DAT at cfgdevice port *nn*-6; SCSI Target 5)
IOU Slot 7	*xx*-0	*xx*-3	pci@*x*7,700000	

* *xx* is the XSB number, in the range of 00-15.

† *xx* is the XSB number, in the range of 00-15.

‡ *x* is LSB-dependent, and is assigned a value as shown in TABLE A-2.

§ *nn* is the number associated with the PSB to which the DVD or DAT device is attached, as follows: for an M8000 server, *nn* is in the range of 0-3; for an M9000 server, *nn* is in the range of 0-7; for an M9000 server plus expansion unit, *nn* is in the range of 0-15.

Sample `cfgadm` Output and IOU Device Matrix

This section contains:

- Sample output for the command `cfgadm -s "select=class(pci)"` on an *unpopulated* server. As you connect devices, the `cfgadm` output will change to reflect the device type and connection status on your server.
- The device matrix for midrange and for high-end servers, when the IOU is configured as part of a domain. I/O portions of the IOU resources may be in different domains.

SPARC Enterprise M4000 and M5000 Servers

SPARC Enterprise M4000 Server sample output:

```
# cfgadm -s "select=class(pci)"
Ap_Id                          Type         Receptacle   Occupant     Condition
iou#0-pci#0                    unknown       empty        unconfigured unknown
iou#0-pci#1                    unknown       empty        unconfigured unknown
iou#0-pci#2                    unknown       empty        unconfigured unknown
iou#0-pci#3                    unknown       empty        unconfigured unknown
iou#0-pci#4                    unknown       empty        unconfigured unknown
```

SPARC Enterprise M5000 Server sample output:

```
# cfgadm -s "select=class(pci)"
Ap_Id                          Type         Receptacle   Occupant     Condition
iou#0-pci#0                     unknown      empty        unconfigured unknown
iou#0-pci#1                     unknown      empty        unconfigured unknown
iou#0-pci#2                     unknown      empty        unconfigured unknown
iou#0-pci#3                     unknown      empty        unconfigured unknown
iou#0-pci#4                     unknown      empty        unconfigured unknown
iou#1-pci#0                     unknown      empty        unconfigured unknown
iou#1-pci#1                     unknown      empty        unconfigured unknown
iou#1-pci#2                     unknown      empty        unconfigured unknown
iou#1-pci#3                     unknown      empty        unconfigured unknown
iou#1-pci#4                     unknown      empty        unconfigured unknown
```

TABLE A-8 `cfgadm` Device Matrix for Midrange Servers

PCI Slot #	PCI Slot Type	IOU#0 (M4000/M5000)	IOU#1 (M5000)
0	PCI-X	iou#0-pci#0	iou#1-pci#0
1	PCIe	iou#0-pci#1	iou#1-pci#1
2	PCIe	iou#0-pci#2	iou#1-pci#2
3	PCIe	iou#0-pci#3	iou#1-pci#3
4	PCIe	iou#0-pci#4	iou#1-pci#4

SPARC Enterprise M8000 and M9000 Servers

SPARC Enterprise M8000 Server sample output:

```
# cfgadm -s "select=class(pci)"
Ap_Id                          Type         Receptacle   Occupant     Condition
iou#1-pci#0                     unknown      empty        unconfigured unknown
iou#1-pci#1                     unknown      empty        unconfigured unknown
iou#1-pci#4                     unknown      empty        unconfigured unknown
iou#1-pci#5                     unknown      empty        unconfigured unknown
iou#1-pci#6                     unknown      empty        unconfigured unknown
iou#1-pci#7                     unknown      empty        unconfigured unknown
```

SPARC Enterprise M9000 Server sample output:

```
# cfgadm -s "select=class(pci)"
Ap_Id                          Type         Receptacle   Occupant     Condition
iou#0-pci#0                    unknown      empty        unconfigured unknown
iou#0-pci#1                    unknown      empty        unconfigured unknown
iou#0-pci#2                    unknown      empty        unconfigured unknown
iou#0-pci#3                    unknown      empty        unconfigured unknown
iou#0-pci#4                    unknown      empty        unconfigured unknown
iou#0-pci#5                    unknown      empty        unconfigured unknown
iou#0-pci#6                    unknown      empty        unconfigured unknown
iou#0-pci#7                    unknown      empty        unconfigured unknown
iou#3-pci#0                    unknown      empty        unconfigured unknown
iou#3-pci#1                    unknown      empty        unconfigured unknown
iou#3-pci#2                    unknown      empty        unconfigured unknown
iou#3-pci#3                    unknown      empty        unconfigured unknown
```

TABLE A-9 `cfgadm` Device Matrix for High-End Servers

PCI Slot #	PCI Slot Type	IOU#0	IOU#1	IOU#*n**
0	PCIe	iou#0-pci#0	iou#1-pci#0	iou#*n*-pci#0
1	PCIe	iou#0-pci#1	iou#1-pci#1	iou#*n*-pci#1
2	PCIe	iou#0-pci#2	iou#1-pci#2	iou#*n*-pci#2
3	PCIe	iou#0-pci#3	iou#1-pci#3	iou#*n*-pci#3
4	PCIe	iou#0-pci#4	iou#1-pci#4	iou#*n*-pci#4
5	PCIe	iou#0-pci#5	iou#1-pci#5	iou#*n*-pci#5
6	PCIe	iou#0-pci#6	iou#1-pci#6	iou#*n*-pci#6
7	PCIe	iou#0-pci#7	iou#1-pci#7	iou#*n*-pci#7

* *n* is the IOU number.

Glossary

audit The collection of data about the use of system resources. Auditing provides a record of security-related system events.

audit class A grouping of audit events. Audit classes provide a way to select a group of events to audit.

audit event A security-related system action that is audited. Events are grouped into classes.

audit file An audit log where audit records are stored.

audit policy A set of auditing options that an administrator can enable or disable. These options include which events will be recorded and whether to record certain kinds of audit data. The options also include whether to suspend audible actions when the audit trail is full.

audit record Audit data that is stored in an audit file. An audit record describes a single audit event. Each audit record is composed of audit tokens.

audit trail A set of audit logs that have been recorded by the server. The audit trail can be analyzed with the use of audit tools.

authentication A method by which a server validates and authorizes a user or function to access or use the server.

authorization The ability to perform an operation, act, or function with a computer resource (for example, run, modify, or show).

The means by which the ability is explicitly enabled or restricted in some way.

Capacity on Demand (COD) An option that provides additional CPU processing resources when needed. These additional CPUs are provided on COD CPU boards that are installed in the server. To access the COD CPUs, you must purchase the COD right-to use (RTU) licenses for them.

COD See Capacity on Demand (COD).

domain A set of one or more system boards that acts as a separate system capable of booting the operating system and running an operating system independently of any other domains. Domains that share a system are characteristically independent of each other.

Each domain is based on the logical system board that is assigned to it. Further, each domain is electrically isolated into hardware partitions, which ensures that any failure in one domain does not affect the other domains in the server.

Domain - SP Communication Protocol (DSCP) Protocol which provides a user-level to user-level TCP/IP sockets type communication between the Service Processor and a domain. This communication occurs over a mailbox type of communication provided by other software components.

DSCP See Domain - SP Communication Protocol (DSCP).

dynamic reconfiguration (DR) Enables logical attachment and detachment of system boards to and from the system without causing system downtime. This is the process of physically installing or removing a system board while the Solaris OS is running.

Enables boards to be electrically isolated (`deleteboard`) from a domain so they can be physically removed from the system or added to a different domain; or to be electrically reattached (`addboard`) so they can be inserted into a running server or assigned to a different domain.

environmental monitoring The monitoring done through a large number of sensors that monitor temperature, voltage, and current. The Service Processor software polls devices in a timely manner and makes the environmental data available. The Service Processor shuts down various components to prevent damage.

eXtended system board (XSB) eXtended System Board combines the hardware resources of a physical system board. The SPARC Enterprise servers can generate one or four XSB(s) from one physical system board: Uni-XSB and Quad-XSB.

eXtended System Control Facility (XSCF) The software that runs on the Service Processor and provides control and monitoring functions for the system platform.

failover Process by which the active Service Processor transfers control to the standby Service Processor or the standby Service Processor takes control over from the active Service Processor. In either case, the previously standby Service Processor becomes the active and the active Service Processor becomes the standby.

field-replaceable unit (FRU) A part that can be replaced by field engineers when servicing the server.

FRU See field-replaceable unit (FRU).

hostid Unique system identifier.

I/O unit (IOU) The I/O unit, which is common to midrange and high-end servers, monitors I/O events and supports PCIe. Further, the midrange server supports PCI-X cards. The PCI cards must first be inserted in a PCI cassette. The I/O unit for the midrange servers supports up to five PCI cassettes: four PCIe cassettes (upper four slots) and one PCI-X cassette (lowest slot).

Lightweight Directory Access Protocol (LDAP) Protocol for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.

log File containing a record of system activity.

log archive Repository for log files.

logical system board (LSB) The unit of grouping for memory, CPU and I/O, which is visible to software. The physical system board (PSB) or eXtended system board (XSB) assigned with the system board number on the domain is recognized as the logical system board. One domain consists of a maximum of 16 logical system boards. These can be a combination of XSBs and PSBs.

LSB See logical system board (LSB).

privileges Specific permissions granted to users who belong to assigned groups. XSCF users can have any one or more of the following privileges: platform administrator, platform operator, domain administrator, domain operator, user administrator, audit administrator, audit operator, and field engineer privileges.

Quad-XSB The divided system board configured with the hardware resource on a physical system board, which is segmented into four. See eXtended system board.

Service Processor A small system, that operates with an independent processor and directs the system startup, reconfiguration, and fault diagnosis, plus giving access to the domain(s). This is where the system management software (XSCF) runs.

Uni-XSB The system board with the undivided hardware resource on a PSB.

XCP See XSCF Control Package (XCP).

XSCF Control Package (XCP) Runs on the Service Processor and contains XSCF, POST, and OpenBoot PROM firmware.

XSB See eXtended system board (XSB).

XSCF See eXtended System Control Facility (XSCF).

Index

A

addboard command, 52, 57
addcodlicense command, 79, 80
adduser command, 14
altitude, 26
applynetwork command, 20, 31
auditing, 63 to 67

B

back up, domain, 56

C

Capacity on Demand, *see* COD
certificate, 26, 34, 41
cfgadm command, 4, 55, 59, 60, 96
cfgdevice command, 55, 59, 60
Chassis HostID, 77
clock, 23
COD, 75 to 87
  boards, 76
  headroom, 78, 79, 80, 82, 83, 84
  license database, 77
  license violation, 79
  right-to-use (RTU) licenses, 76 to 87
commands
  addboard, 52, 57
  addcodlicense, 79, 80
  adduser, 14
  applynetwork, 20, 31
  cfgadm, 4, 55, 59, 60, 96
  cfgdevice, 55, 59, 60
console, 52, 55, 58
deletecodlicense, 79, 80
password, 14
poweron, 52, 58
prtdiag, 90, 91
rebootxscf, 35
rlogin, 55
rsh, 55
setaltitude, 26, 43
setarchiving, 72, 73
setaudit, 66
setcod, 78, 81, 82, 83
setdate, 23, 36
setdcl, 52, 57, 89
setdscp, 18, 19, 28
sethostname, 20, 21, 32
sethttps, 26, 41
setldap, 23, 34
setlookup, 23, 33
setnameserver, 20, 21, 33
setnetwork, 20, 29
setntp, 34
setpasswordpolicy, 9, 15
setprivileges, 15, 23
setroute, 20, 31
setsmtp, 26, 42
setsnmp, 40
setsnmpusm, 36
setsnmpvacm, 38
setssh, 26, 43
settelnet, 26, 42
settimezone, 35
setupfru, 26, 47, 52, 56
showaltitude, 43

showarchiving, 71, 73
showaudit, 66, 67
showboards, 57, 58, 86, 91
showcod, 82, 83, 84
showcodlicense, 80, 81, 85
showcodusage, 86
showdate, 36
showdcl, 57
showdscp, 19, 24, 28, 29
showfru, 56
showhttps, 41
showldap, 34
showlookup, 33
shownetwork, 30, 31, 32
shownтp, 35
showpasswordpolicy, 15
showsmtp, 26, 42
showsnmp, 40, 41
showsnmpusm, 37
showsnmpvacm, 38, 39
showssh, 43
showtelnet, 42
showtimezone, 36
showuser, 14, 22
snapshot, 71
telnet, 55
version, 16
console
access to a domain, 55, 58
escape character, 58
console command, 52, 55, 58
CPU module, 46, 89

D

DAT drive, 55
date, 23, 34, 35
deletecodlicense command, 79, 80
device path name mapping, 89
DIMMs, 46, 49
DNS, 3, 21, 32 to 33
domain
and COD licenses, 76, 77, 80, 81, 84, 86
backup and restore operations, 56
configuring, 45 to 61
console access to, 55
DCL, 51, 52, 57
DVD or DAT drive, 55
log in, 8, 55
power on, 57
resource assignment, 50
DSCP network, 18 to 19, 55
DVD drive, 55
dynamic reconfiguration, 56

E

escape character, 58
/etc/inet/ntp.conf file, 24
eXtended system board, *see* XSB

F

failover, 2, 10, 18, 20, 21, 25, 77, 78
fault management, 4, 25
FRU ID, 76

H

host name, 21, 32
host public key, 26, 43
hot replacement, 4
HTTPS, 3, 26, 41

I

I/O, 4, 46, 50, 55, 89
IOU (I/O unit), 50, 92
IP address, 4, 18 to 23, 55, 64

K

keyswitch, 12

L

LDAP, 3, 9, 10, 21 to 23, 33 to 34
licenses, COD, *see* COD
log in, 8, 12, 55
logical system board, *see* LSB
logs
archiving, 69
audit, 63
LSB, 51, 57, 89 to 92

M

man pages, 6
see also commands
mapping

CPU, 89
I/O device, 89
memory, 26, 46, 50
MIB, 25, 38
mirrored memory mode, 26
MODE switch, 12

N

netmask, 4, 19
NTP, 3, 23 to 24, 34 to 35, 52
ntp.conf file, 24

P

password
LDAP, 23, 34
lost, 9, 12
policy, 9, 14
XSCF, 9, 14
password command, 14
PCIe slot, 46, 92
poweron command, 52, 58
private key, 26, 41
privileges, 9 to 11, 15
prtdiag command, 90, 91
PSB, 46
public key, 26, 43

R

rebootxscf command, 35
restore, domain, 56
rlogin command, 55
rsh command, 55

S

scp program, 70
security
auditing, 63
authentication, 8, 10
by default, 3
LDAP, 21, 33
MD5 encryption, 23
privileges, 8, 10
public key, 70
SSH, 3, 8, 14, 71
Telnet, 3
UNIX crypt, 23
Service Processor
defined, 2
log in, 8
set date and time, 23, 34, 35
setaltitude command, 26, 43
setarchiving command, 72, 73
setaudit command, 66
setcod command, 78, 81, 82, 83
setdate command, 23, 36
setdcl command, 52, 57, 89
setdscp command, 18, 19, 28
sethostname command, 20, 21, 32
sethttps command, 26, 41
setldap command, 23, 34
setlookup command, 23, 33
setnameserver command, 20, 21, 33
setnetwork command, 20, 29
setntp command, 34
setpasswordpolicy command, 9, 15
setprivileges command, 15, 23
setroute command, 20, 31
setsmtp command, 26, 42
setsnmp command, 40
setsnmpusm command, 36
setsnmpvacm command, 38
setssh command, 26, 43
settelnet command, 26, 42
settimezone command, 35
setupfru command, 26, 47, 52, 56
showaltitude command, 43
showarchiving command, 71, 73
showaudit command, 66, 67
showboards command, 57, 58, 86, 91
showcod command, 82, 83, 84
showcodlicense command, 80, 81, 85
showcodusage command, 86
showdate command, 36
showdcl command, 57
showdscp command, 19, 24, 28, 29
showfru command, 56
showhttps command, 41
showldap command, 34

showlookup command, 33
shownetwork command, 30, 31, 32
shownetwork command, 30, 31, 32
showntp command, 35
showpasswordpolicy command, 15
showsmtp command, 26, 42
showsnmp command, 40, 41
showsnmpusm command, 37
showsnmpvacm command, 38, 39
showssh command, 43
showtelnet command, 42
showtimezone command, 36
showuser command, 14, 22
SMTP, 3, 26
snapshot command, 71
SNMP, 3, 24 to 25, 36 to 41
Solaris OS, 2, 8, 46, 50, 52, 55, 56
SSH, 3, 8, 14, 26, 42, 55, 71
syslog function, 71

T

tape drive, 55
Telnet, 3, 26, 42
telnet command, 55
temperature, 27
time, 23, 34, 35

U

UID number, 14, 22
update, XCP, 11
user
  UID number, 14, 22
  XSCF account, 8 to 15
  XSCF password, 9, 14
  XSCF privileges, 8 to 15
user public key, 43

V

version command, 16
vold daemon, 59, 60

X

XCP image, 2, 11
XSB, 46 to 57, 92
XSCF firmware, defined, 1
XSCF network, 20

FUJITSU